AUTHORIZED DOCUMENTATION

Administration Guide

Novell®
ZENworks® Endpoint Security Management

3.5

March 31, 2009

www.novell.com

Legal Notices

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

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

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

Copyright © 2007-2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

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

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

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.

Contents

About This Guide 9

1 ZENworks Endpoint Security Management 11

1.1 ZENworks Endpoint Security Management Overview 12
1.2 System Requirements 13
1.2.1 ASP.NET 14
1.2.2 Reliable Time Stamp 14
1.3 About the ZENworks Endpoint Security Management Manuals. 14
1.4 USB/Wireless Security 14

2 Policy Distribution Service 17

2.1 About the Policy Distribution Service 17
2.1.1 Server Selection and Installation 18
2.1.2 Server Maintenance. 18
2.1.3 Upgrading the Software 18
2.1.4 Uninstall 18
2.2 Securing Server Access. 18
2.2.1 Physical Access Control 18
2.2.2 Network Access Control 19
2.2.3 High Availability 19
2.3 Running the Service. 19

3 Configuring the Directory Service 21

3.1 Configuring the Directory Service for Novell eDirectory. 21
3.2 Configuring the Directory Service for Microsoft Active Directory 28

4 Using the ZENworks Endpoint Security Management Service 37

4.1 About the Management Service. 37
4.1.1 Server Selection and Installation 37
4.1.2 Server Maintenance. 38
4.1.3 Upgrading the Software 38
4.1.4 Uninstall 38
4.2 Securing Server Access. 38
4.2.1 Physical Access Control 38
4.2.2 Network Access Control 39
4.2.3 High Availability 39
4.2.4 Running the Service 39
4.3 Distributing and Renewing ZENworks Endpoint Security Management Credentials 39
4.3.1 Distributing Endpoint Security Management Credentials (Key Management Key) . . 39
4.3.2 Periodic Renewal of the Key Management Key (KMK) 40

5 Using the ZENworks Storage Encryption Solution Management Console 41

5.1 Using the Console Taskbar 41
5.1.1 Policy Tasks. 42
5.1.2 Resources 43

5.1.3 Configuration 43
5.1.4 Endpoint Auditing. 43
5.2 Using the Console Menu Bar 43
5.3 Using the Configuration Window 44
5.3.1 Infrastructure and Scheduling 44
5.3.2 Authenticating Directories 46
5.3.3 Service Synchronization 47
5.4 Using Alerts Monitoring 47
5.4.1 Configuring Endpoint Security Management for Alerts 48
5.4.2 Configuring Alert Triggers 49
5.4.3 Managing Alerts. 50
5.5 Using Reports 51
5.5.1 Using the Reports Tools 51
5.5.2 Adherence Reports 53
5.5.3 Alert Drill-Down Reports 55
5.5.4 Application Control Reports 56
5.5.5 Endpoint Activity Reports. 56
5.5.6 Encryption Solutions Reports 57
5.5.7 Client Self Defense Reports 57
5.5.8 Integrity Enforcement Reports 57
5.5.9 Location Reports 58
5.5.10 Outbound Content Compliance Reports 58
5.5.11 Administrative Overrides Reports 59
5.5.12 Endpoint Updates Reports. 59
5.5.13 USB Devices Reports 60
5.5.14 Wireless Enforcement Reports 60
5.6 Generating Custom Reports 60
5.6.1 Software Requirements 61
5.6.2 Creating a ZENworks Endpoint Security Management Compliant Report. 61
5.6.3 Available Reporting Information. 62
5.6.4 Creating a Report 65
5.7 Using the ZENworks Storage Encryption Solution. 71
5.7.1 Understanding the ZENworks Storage Encryption Solution 71
5.7.2 Sharing Encrypted Files. 71
5.8 Managing Keys 72
5.8.1 Exporting Encryption Keys. 73
5.8.2 Importing Encryption Keys. 74
5.8.3 Generating a New Key. 74

6 Creating and Distributing Security Policies 75

6.1 Navigating the Management Console UI 75
6.1.1 Using the Policy Tabs and Tree. 76
6.1.2 Using the Policy Toolbar 78
6.2 Creating Security Policies 79
6.2.1 Global Policy Settings 80
6.2.2 Locations 98
6.2.3 Integrity and Remediation Rules 109
6.2.4 Compliance Reporting 118
6.2.5 Publishing Security Policies. 121
6.3 Managing Policies 122
6.3.1 Show Usage 122
6.3.2 Error Notification 122
6.3.3 Custom User Messages 123
6.3.4 Hyperlinks 124
6.3.5 Defined Location Settings 125
6.3.6 Network Environments. 126

6.3.7 Firewall Settings 128
6.3.8 TCP/UDP Ports 130
6.3.9 Access Control Lists 134
6.3.10 Application Controls. 136
6.3.11 Rule Scripting Parameters. 138
6.4 Importing and Exporting Policies 169
6.4.1 Importing Policies 169
6.4.2 Exporting a Policy 169
6.4.3 Exporting Policies to Unmanaged Users 169
6.5 Sample Scripts 170
6.5.1 Create Registry Shortcut (VB Script) 170
6.5.2 Allow Only One Connection Type (JScript) 172
6.5.3 Stamp Once Script. 173

7 Managing the Endpoint Security Client 3.5 175

7.1 Understanding the Endpoint Security Client 175
7.2 Installing and Uninstalling the ZENworks Security Agent. 176
7.2.1 Installing the Endpoint Security Client 3.5 176
7.2.2 Uninstalling the Endpoint Security Client 3.5. 176
7.3 Understanding Client Self Defense 177
7.4 Upgrading the Endpoint Security Client 3.5 178
7.4.1 Setting the Upgrade Switch 178
7.5 Running the Endpoint Security Client 3.5 178
7.5.1 Multiple User Support 179
7.5.2 Machine-Based Policies (Active Directory Only) 179
7.5.3 Distributing Unmanaged Policies. 179
7.6 Using the Endpoint Security Client Diagnostics Tools 180
7.6.1 Creating a Diagnostics Package 180
7.6.2 Administrator Views. 182
7.6.3 Logging 186
7.6.4 Reporting 187

8 Managing the Endpoint Security Client 4.0 191

8.1 Understanding the Endpoint Security Client 191
8.2 Installing and Uninstalling the ZENworks Security Agent. 192
8.2.1 Installing the Endpoint Security Client 4.0 192
8.2.2 Uninstalling the Endpoint Security Client 4.0. 192
8.3 Running the Endpoint Security Client 4.0 193
8.3.1 Multiple User Support 194
8.3.2 Machine-Based Policies (Active Directory Only) 194
8.3.3 Distributing Unmanaged Policies. 195
8.4 Using the Endpoint Security Client Diagnostics Tools 195
8.4.1 Creating a Diagnostics Package 195
8.4.2 Administrator Views. 197
8.4.3 Module List 200
8.4.4 Logging 201

9 Using ZENworks Endpoint Security Management Utilities 203

9.1 Using the ZENworks File Decryption Utility 203
9.1.1 Using the File Decryption Utility. 203
9.1.2 Using the Administrator Configured Decryption Utility. 204
9.2 Using the Override-Password Key Generator 204

A Acronym Glossary 207

About This Guide

This *Novell® ZENworks® Endpoint Security Management Administration Guide* is written for ZENworks Endpoint Security Management Administrators who are required to manage the Endpoint Security Management 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.

The information in this guide is organized as follows:

- Chapter 1, "ZENworks Endpoint Security Management," on page 11
- Chapter 2, "Policy Distribution Service," on page 17
- Chapter 3, "Configuring the Directory Service," on page 21
- Chapter 4, "Using the ZENworks Endpoint Security Management Service," on page 37
- Chapter 5, "Using the ZENworks Storage Encryption Solution Management Console," on page 41
- Chapter 6, "Creating and Distributing Security Policies," on page 75
- Chapter 7, "Managing the Endpoint Security Client 3.5," on page 175
- Chapter 8, "Managing the Endpoint Security Client 4.0," on page 191
- Chapter 9, "Using ZENworks Endpoint Security Management Utilities," on page 203
- Appendix A, "Acronym Glossary," on page 207

Audience

This guide is written for the ZENworks Endpoint Security Management administrators.

Feedback

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

Additional Documentation

ZENworks Endpoint Security Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks Endpoint Security Management 3.5 documentation Web site (http://www.novell.com/documentation/zesm35).

Documentation Conventions

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

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

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux*, should use forward slashes as required by your software.

ZENworks Endpoint Security Management

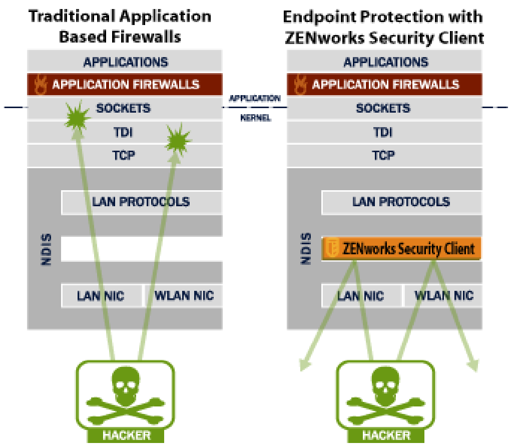
1

Novell® ZENworks® Endpoint Security Management provides complete, centralized security management for all endpoints in the enterprise. Because ZENworks Endpoint Security Management applies security at the most vulnerable point, the endpoint, all security settings are applied and enforced regardless of whether the user is connecting to the network directly, dialing in remotely, or even not connecting to corporate infrastructure at all. This is critical to not only protect the data within the corporate perimeter, but also to protect the critical data that resides on the endpoint device itself.

ZENworks Endpoint Security Management automatically adjusts security settings and user permissions based on the current network environment characteristics. A sophisticated engine is used to determine the user's location and automatically adjusts firewall settings and permissions for applications, adapters, hardware, etc.

Security is enforced through the creation and distribution of ZENworks Endpoint Security Management security policies. Each location (Work, Home, Alternate, Airport, etc.) listed in a security policy is assigned to a network environment (or multiple network environments). A location determines which hardware is available and the degree of firewall settings that are activated within the network environment. The firewall settings determine which networking ports, access control lists (ACLs), and applications are accessible/required. Various integrity checks and scripts can be run at location change to ensure that all required security software is up to date and running.

Figure 1-1 *Effectiveness of NDIS-Layer Firewall*



In securing mobile devices, ZENworks Endpoint Security Management is superior to typical personal firewall technologies, which operate only in the application layer or as a firewall-hook driver. ZENworks Endpoint Security Management client security is integrated into the Network Driver Interface Specification (NDIS) driver for each network interface card (NIC), providing security protection from the moment traffic enters the computer. Differences between ZENworks Endpoint Security Management and application-layer firewalls and filter drivers are illustrated in Figure 1-1, "Effectiveness of NDIS-Layer Firewall," on page 11.

Security decisions and system performance are optimized when security implementations operate at the lowest appropriate layer of the protocol stack. With the ZENworks Security Management Endpoint Security Client, unsolicited traffic is dropped at the lowest levels of the NDIS driver stack by means of Adaptive Port Blocking (stateful packet inspection) technology. This approach protects against protocol-based attacks, including unauthorized port scans, SYN Flood, NetBIOS, and DDOS attacks.

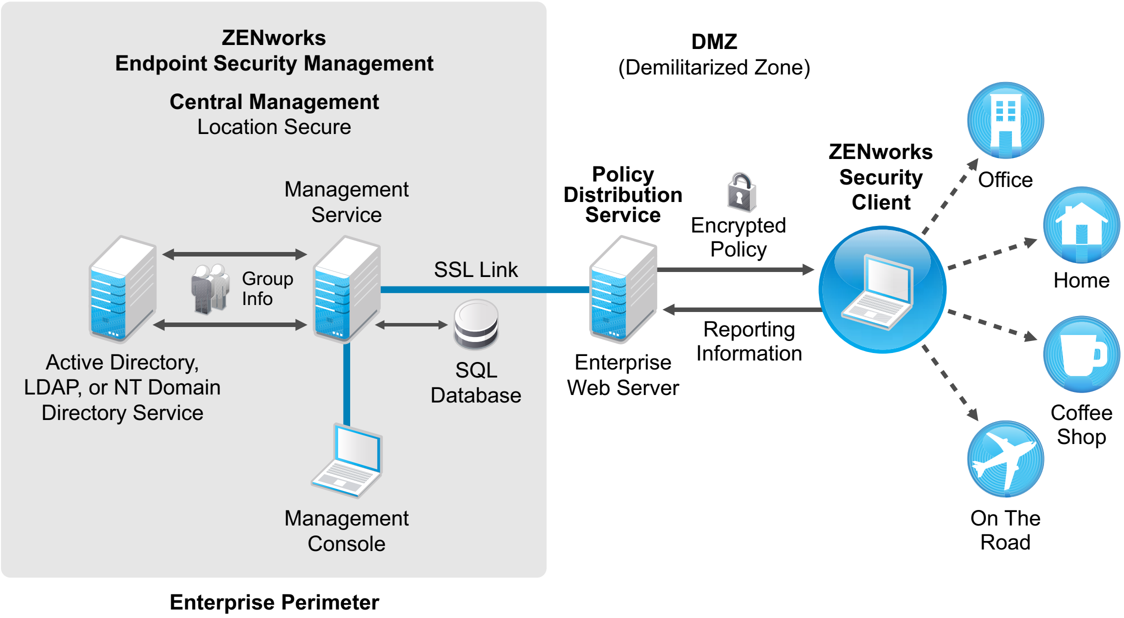
1.1 ZENworks Endpoint Security Management Overview

ZENworks Endpoint Security Management consists of four high-level functional components:

- Policy Distribution Service
- Management Service
- Management Console
- Endpoint Security Client

The figure below shows these components in the architecture:

Figure 1-2 *ZENworks Endpoint Security Management Architecture*



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

Each Central Management component is installed separately, the following components are installed on servers that are secured inside the corporate perimeter:

- **Policy Distribution Service:** Responsible for the distribution of security policies to the Endpoint Security Client, and retrieval of reporting data from the Endpoint Security Clients. The Policy Distribution Service can be deployed in the DMZ or outside the enterprise firewall, to ensure regular policy updates for mobile endpoints.
- **Management Service:** Responsible for user policy assignment and component authentication; reporting data retrieval, creation and dissemination of ZENworks Endpoint Security Management reports; and security policy creation and storage.
- **Management Console:** The 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 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 Management Console.

1.2 System Requirements

Server System Requirements	Client System Requirements
Operating Systems: Microsoft* Windows* 2003 Server **Processor:** 3.0 GHz Pentium* 4 HT (or greater) 756 MB RAM minimum (1 GB+ Recommended) **Disk Space:** 500 MB - Without local Microsoft SQL database 5 GB - With local MS SQL database (SCSI recommended) **Required Software:** Supported RDBMS (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, or SQL 2005) Microsoft Internet Information Services (configured for SSL) Supported Directory Services (eDirectory, Active Directory, or NT Domains*) .NET framework 3.5 (servers and Management Control only) **Standalone Management Control:** Supported RDBMS (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005, SQL Express)	**Operating Systems for Endpoint Security Client 3.5:** Windows XP SP1 Windows XP SP2 Windows 2000 SP4 **Operating Systems for Endpoint Security Client 4.0**: Windows Vista SP1 (32-bit) **Processor:** 600MHz Pentium 3 (or greater) Minimum 128 MB RAM (256 MB or greater recommended **Disk Space:** 5 MB required, 5 additional MB recommended for reporting data **Required Software:** Windows 3.1 Installer All Windows updates should be current

1.2.1 ASP.NET

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

1.2.2 Reliable Time Stamp

The Novell ZENworks Endpoint Security Management solution gathers data from multiple sources and collates this data to create a wide variety of security and audit reports. The utility and probative value of these reports is greatly diminished if disparate sources disagree as to times, and so it is strongly recommended that anyone installing ZENworks Endpoint Security Management provide for enterprise-wide time synchronization (such as that provided by Active Directory* or through the use of Network Time Protocol).

ZENworks Endpoint Security Management Administrators should follow all installation, operation, and maintenance recommendations provided in this document and the *ZENworks Endpoint Security Management Installation Guide* in order to ensure a strong security environment.

1.3 About the ZENworks Endpoint Security Management Manuals

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

- *ZENworks Endpoint Security Management Administration Guide:* This guide is written for the ZENworks Endpoint Security Management Administrators who manage the ZENworks Endpoint Security Management services, create security policies for the enterprise, generate and analyze reporting data, and provide troubleshooting for users. Instructions for completing these tasks are provided in this manual. This is the guide you are currently reading.
- *ZENworks Endpoint Security Management Installation Guide*: This guide provides complete installation instructions for the ZENworks Endpoint Security Management components and assists the administrator in getting those components up and running.
- *ZENworks Endpoint Security Client 3.5 User Guide*: This manual is written to instruct the end user on the operation of the Endpoint Security Client running on Windows XP and Windows 2000. This guide can be sent to all employees in the enterprise to help them understand how to use the Endpoint Security Client.
- *ZENworks Endpoint Security Client 4.0 User Guide*: This manual is written to instruct the end user on the operation of the Endpoint Security Client running on Windows Vista. This guide can be sent to all employees in the enterprise to help them understand how to use the Endpoint Security Client.

1.4 USB/Wireless Security

ZENworks USB/Wireless Security (UWS) is a simplified version of the product that provides comprehensive USB control, connectivity security, and file encryption features. ZENworks USB/Wireless Security does not include some of the additional security features that are available in ZENworks Endpoint Security Management. If you have purchased USB/Wireless Security rather than ZENworks Endpoint Security Management, all functionality described in this manual will be essentially the same, with only certain policy features unavailable in the Management Console.

The unavailable features have been marked with the following notation on their respective pages:

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for USB/Wireless Security security policies.

Features without this notation are available for both ZENworks Endpoint Security Management and UWS security policies.

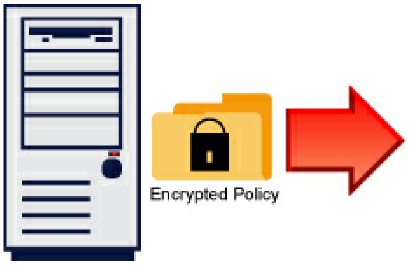
To verify which version you are running, open the "About" screen from the Help menu in Management Console (see Section 5.2, "Using the Console Menu Bar," on page 43).

Policy Distribution Service

2

The Policy Distribution Service in Novell® ZENworks® Endpoint Security Management is a web service application that, when requested, distributes security policies and other necessary data to Endpoint Security Clients on endpoint computers in your enterprise. Endpoint Security Management security policies are created and edited with the Management Service's Management Console, then published to the Policy Distribution Service, from where they are downloaded by the client at check-in.

The following graphic illustrates the role of the Policy Distribution Service:



The following sections contain additional information:

- Section 2.1, “About the Policy Distribution Service,” on page 17
- Section 2.2, “Securing Server Access,” on page 18
- Section 2.3, “Running the Service,” on page 19

2.1 About the Policy Distribution Service

The Policy Distribution Service authenticates Endpoint Security Clients based on the user ID credentials obtained from the Management Service, and supplies each client with the designated security policy.

Reporting data is collected by Endpoint Security Clients and passed up to the Policy Distribution Service. This data is periodically collected by the Management Service and then deleted from the Policy Distribution Service.

The Policy Distribution Service does not initiate any communications with the other Endpoint Security Management components, and only responds to others. It does not hold sensitive data in the clear, nor does it hold the keys needed to decrypt the sensitive data. It does not hold user credentials or any other user-specific data.

- Section 2.1.1, “Server Selection and Installation,” on page 18
- Section 2.1.2, “Server Maintenance,” on page 18
- Section 2.1.3, “Upgrading the Software,” on page 18
- Section 2.1.4, “Uninstall,” on page 18

2.1.1 Server Selection and Installation

See the *ZENworks Endpoint Security Management Installation Guide* for selection and installation instructions.

2.1.2 Server Maintenance

It is recommended that regular disk cleanup tasks be configured to run on this server to remove temporary files from the `Windows\temp` folder. Under extreme load conditions, Windows can generate an inordinate amount of temporary files that needlessly consume disk space.

2.1.3 Upgrading the Software

To upgrade your software from one release to another, you must uninstall the old release and install the new release. Complete instructions are provided in "Upgrading" in the *ZENworks Endpoint Security Management Installation Guide*.

2.1.4 Uninstall

To uninstall the Policy Distribution Service, use the Add/Remove Programs function in the Windows Control Panel, or run the installation again from the ZENworks Endpoint Security Management installation CD.

2.2 Securing Server Access

The following sections contain information to help you secure access to your ZENworks Endpoint Security Management server:

- Section 2.2.1, "Physical Access Control," on page 18
- Section 2.2.2, "Network Access Control," on page 19
- Section 2.2.3, "High Availability," on page 19

2.2.1 Physical Access Control

Physical access to the Distribution Service Server should be controlled to prevent access by unauthorized parties. Measures taken should be appropriate to the risks involved. There are multiple available standards and guidelines available, including NIST recommendations, HIPAA requirements, ISO/IEC 17799, and less formal collections of recommendations such as CISSP or SANS guidelines. Even when a given regulatory frameworks is not applicable, it may still act as a valuable resource and planning guide.

Likewise, Disaster Recovery and Business Continuity mechanisms to protect the Distribution Server should be put in place to protect the server if an organizational risk assessment identifies a need for such steps. The mechanisms best used will depend on the specifics of the organization and its desired risk profile, and cannot be described in advance. The same standards and guidelines sources listed above can be helpful in this decision as well.

2.2.2 Network Access Control

The Distribution Server can be further protected from unauthorized access by restricting network access to it. This may take the form of some or all of the following:

- Restricting incoming connection attempts to those ports and protocols from which a valid access attempt might be expected
- Restricting outgoing connection attempts to those IP addresses to which a valid access attempt might be expected
- Restricting outgoing connection attempts to those ports and protocols to which a valid access attempt might be expected

Such measures can be imposed through the use of standard firewall technology.

2.2.3 High Availability

High Availability mechanisms for the Distribution Server should be put in place if an organizational risk assessment identifies a need for such steps. There are multiple alternative mechanisms for building high availability solutions, ranging from the general (DNS round-robining, layer 3 switches, etc.) to the vendor specific (the Microsoft* web site has multiple resources on high availability web services and clustering issues). Those implementing and maintaining a ZENworks Endpoint Security Management solution should determine which class of high availability solution is most appropriate for their context. Note that the Distribution Server has been architected to function in non-high-availability situations, and does not require High Availability to provide its services.

2.3 Running the Service

The Policy Distribution Service launches immediately following installation, with no reboot of the server required. The Management Console can adjust upload times for the Distribution Service using the Configuration feature (see Section 5.3.1, “Infrastructure and Scheduling,” on page 44).

Configuring the Directory Service 3

After you install ZENworks® Endpoint Security Management, you must create and configure a directory service before you can start managing devices in your system.

The New Directory Service Configuration Wizard lets you create a directory service configuration that defines the scope of your ZENworks Endpoint Security Management client installations. The new configuration uses your existing directory service to define the logical boundary for your user-based and computer-based client installations.

The wizard guides you through the process of selecting the directory service and the containers where current and future client accounts reside.

The wizard also lets you synchronize the directory entries included in the new configuration. This synchronization is performed in the background so you can immediately begin using your new configuration.

The following sections contain more information:

- Section 3.1, "Configuring the Directory Service for Novell eDirectory," on page 21
- Section 3.2, "Configuring the Directory Service for Microsoft Active Directory," on page 28

3.1 Configuring the Directory Service for Novell eDirectory

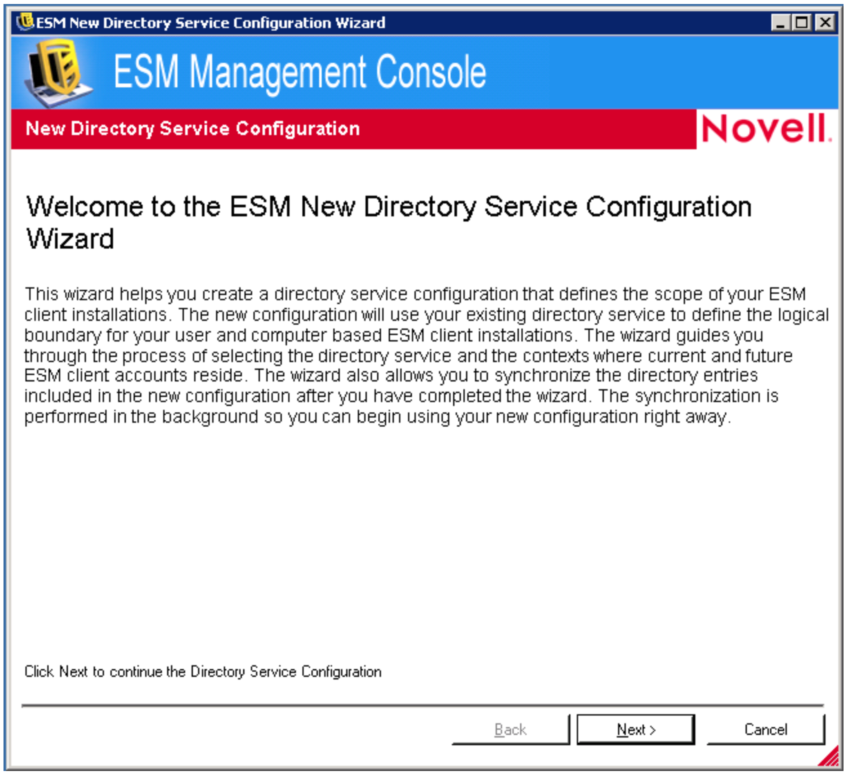
After installing ZENworks Endpoint Security Management, the New Directory Service Configuration Wizard automatically displays. If you have just installed the product and the Welcome page is displayed, skip to Step 4 in the following procedure.

To configure the directory service:

1 In the Management Console, click *Tools* > *Configuration*.

2 Click *Authenticating Directories*.

3 Click *New* to launch the New Directory Service Configuration Wizard.

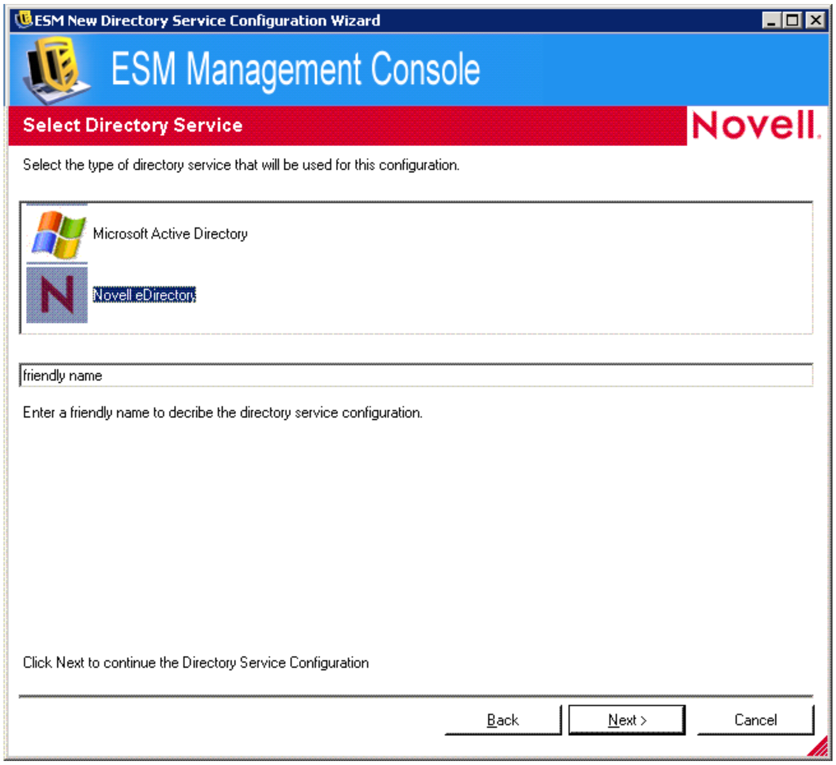

ESM New Directory Service Configuration Wizard
ESM Management Console
New Directory Service Configuration
Novell.

Welcome to the ESM New Directory Service Configuration Wizard

This wizard helps you create a directory service configuration that defines the scope of your ESM client installations. The new configuration will use your existing directory service to define the logical boundary for your user and computer based ESM client installations. The wizard guides you through the process of selecting the directory service and the contexts where current and future ESM client accounts reside. The wizard also allows you to synchronize the directory entries included in the new configuration after you have completed the wizard. The synchronization is performed in the background so you can begin using your new configuration right away.

Click Next to continue the Directory Service Configuration

4 Click *Next* to display the Select Directory Service page.



Select the type of directory service that will be used for this configuration.

Microsoft Active Directory

Novell eDirectory

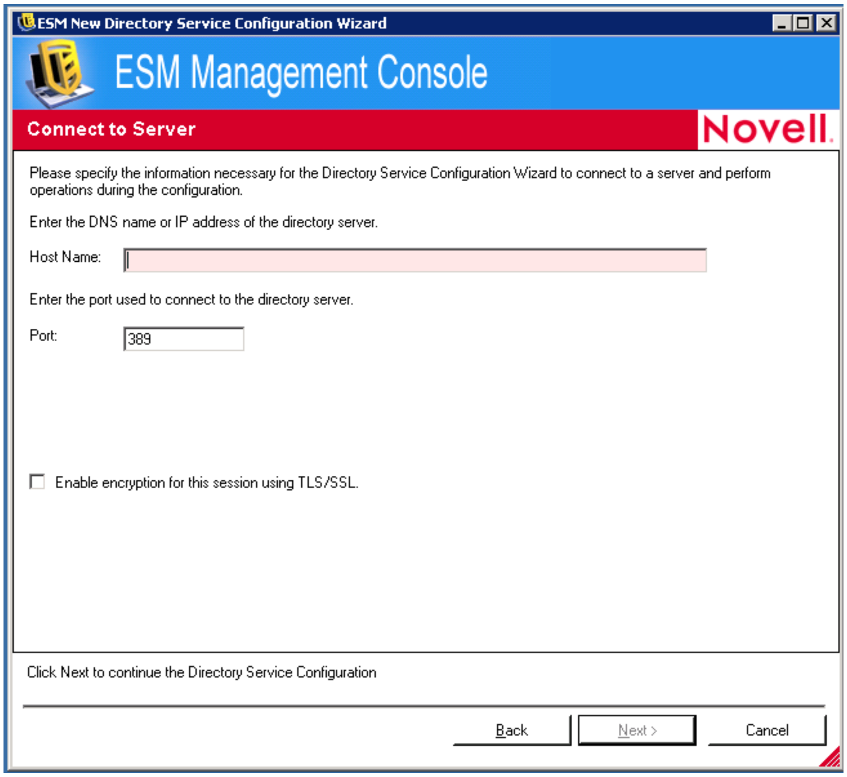
friendly name

Enter a friendly name to decribe the directory service configuration.

Click Next to continue the Directory Service Configuration

5 Select *Novell eDirectory* as the directory service.

6 Specify a friendly name to describe the directory service configuration, then click *Next* to display the Connect to Server page.



Please specify the information necessary for the Directory Service Configuration Wizard to connect to a server and perform operations during the configuration.

Enter the DNS name or IP address of the directory server.

Host Name:

Enter the port used to connect to the directory server.

Port: 389

□ Enable encryption for this session using TLS/SSL.

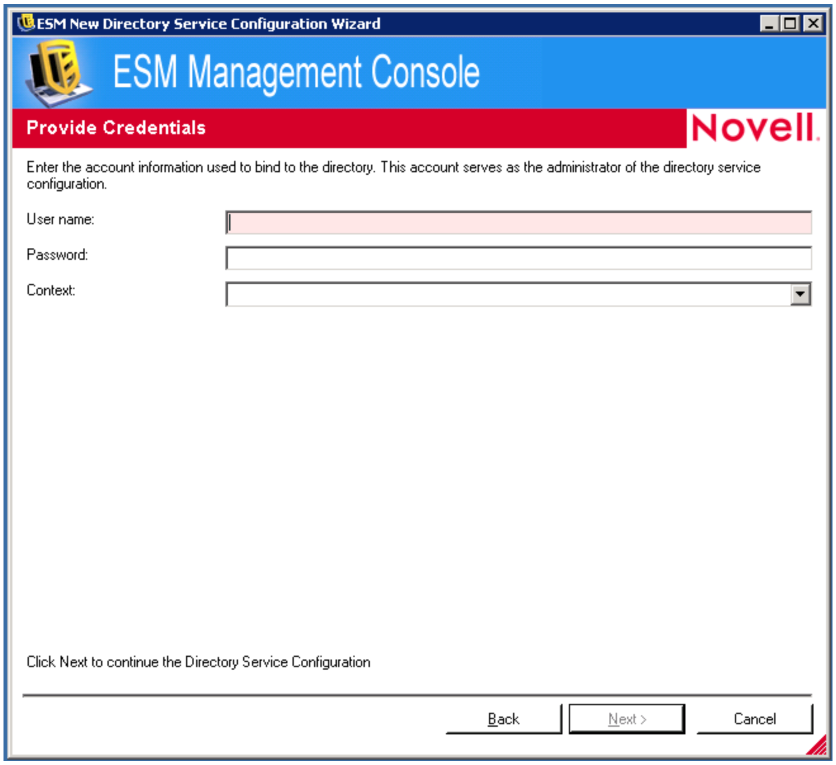
Click Next to continue the Directory Service Configuration

7 Fill in the fields:

- **Host Name:** Specify the DNS name or IP address of the directory server. If the DNS name or IP address cannot be authenticated, a bind error message displays.
- **Port:** Specify the port used to connect to the directory server.

  Port 389 is the default. If you use a different port to connect to the directory server, you can specify that port.
- **Enable Encryption for this Session using TLS/SSL:** Select to enable encryption. If you select this option, the port is automatically changed to 636.

8 Click *Next* to display the Provide Credentials page.



Enter the account information used to bind to the directory. This account serves as the administrator of the directory service configuration.

User name:

Password:

Context:

Click Next to continue the Directory Service Configuration

9 Fill in the fields:

- **User name:** Specify the account administrator to bind to the directory.

  This account serves as the administrator of the directory service configuration. The login name must be a user who has permission to view the entire directory tree. It is recommended that this user be the OU administrator.

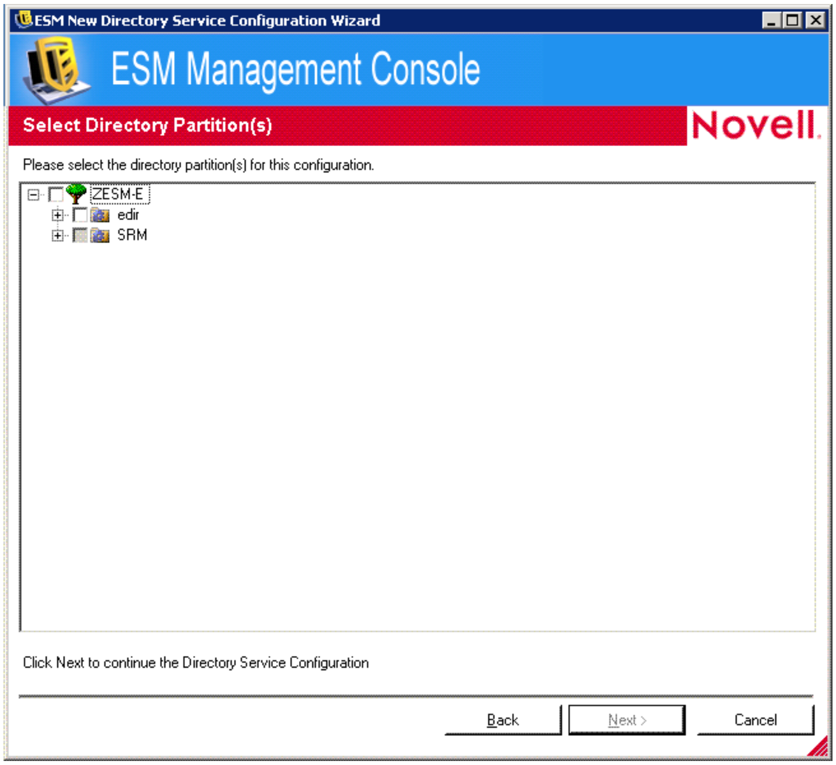
- **Password:** Specify the password for the account administrator.

  This account serves as the administrator of this directory service configuration.

  The password should not be set to expire, and this account should never be disabled.

- **Context:** Specify the context in which the account administrator is a member.

10 Click *Next* to display the Select Directory Partitions page.



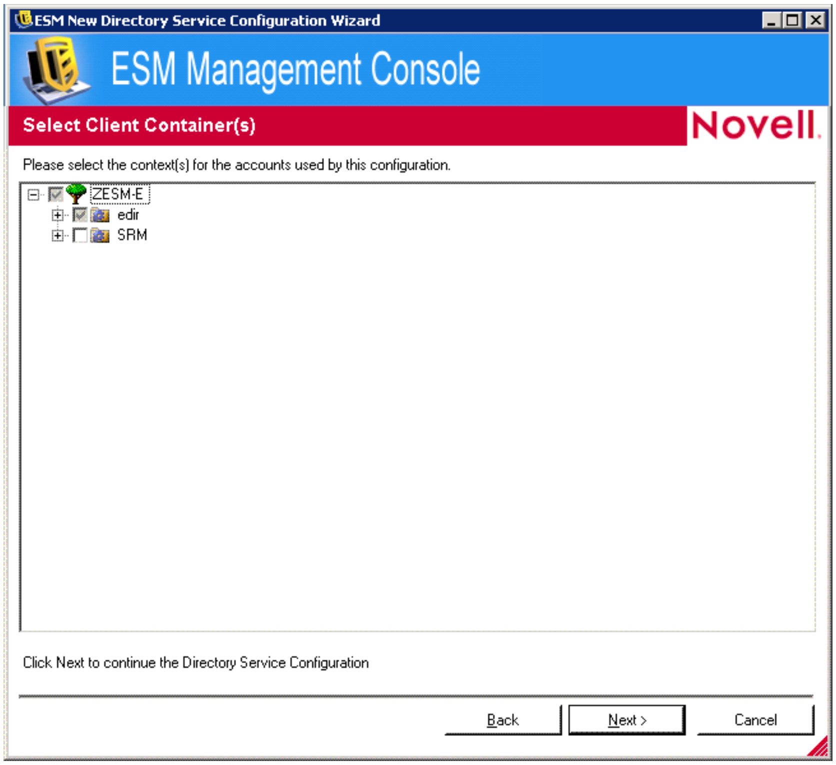
Select Directory Partition(s)

Please select the directory partition(s) for this configuration.

- □ ZESM-E
  - □ edir
  - □ SRM

Click Next to continue the Directory Service Configuration

11 Browse to and select the directory partitions for this configuration, then click *Next* to display the Select Client Contexts page.



Select Client Container(s)

Please select the context(s) for the accounts used by this configuration.

- ☑ ZESM-E
  - ☑ edir
  - □ SRM

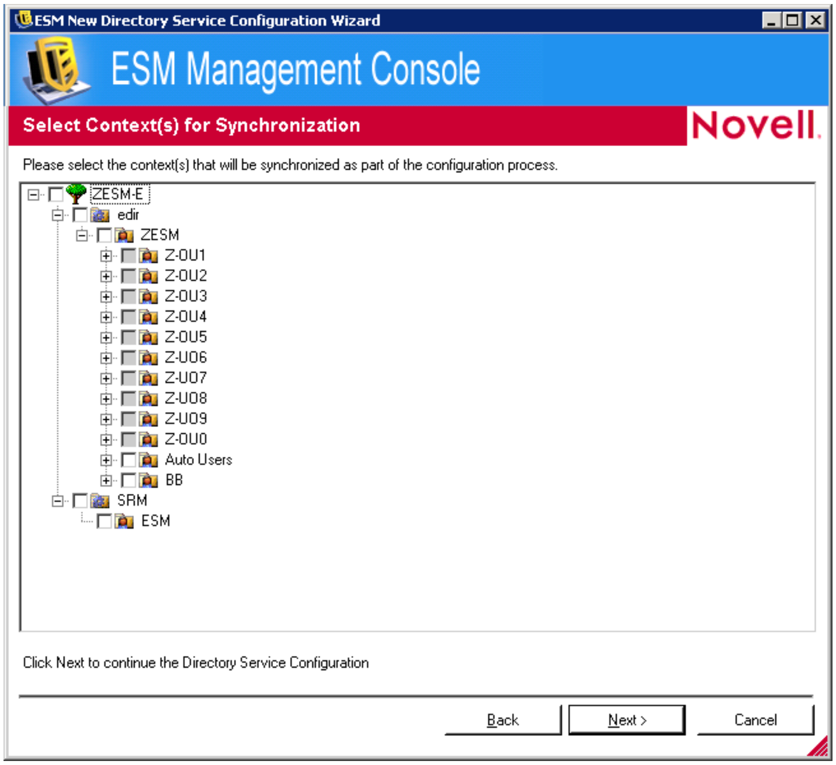
Click Next to continue the Directory Service Configuration

12 Browse to and select the context(s) for the accounts used in this configuration.

The Select Client Context(s) page lets you narrow the search to only those contexts that contain managed users and computers, which improves performance.

Any client installation that attempts to check in with the management server the does not reside in a selected context results in longer search times.

13 Click *Next* to display the Select Context(s) for Synchronization page.



Select Context(s) for Synchronization

Please select the context(s) that will be synchronized as part of the configuration process.

- □ ZESM-E
  - □ edir
    - □ ZESM
      - □ Z-OU1
      - □ Z-OU2
      - □ Z-OU3
      - □ Z-OU4
      - □ Z-OU5
      - □ Z-U06
      - □ Z-U07
      - □ Z-U08
      - □ Z-U09
      - □ Z-OU0
      - □ Auto Users
      - □ BB
  - □ SRM
    - □ ESM

Click Next to continue the Directory Service Configuration

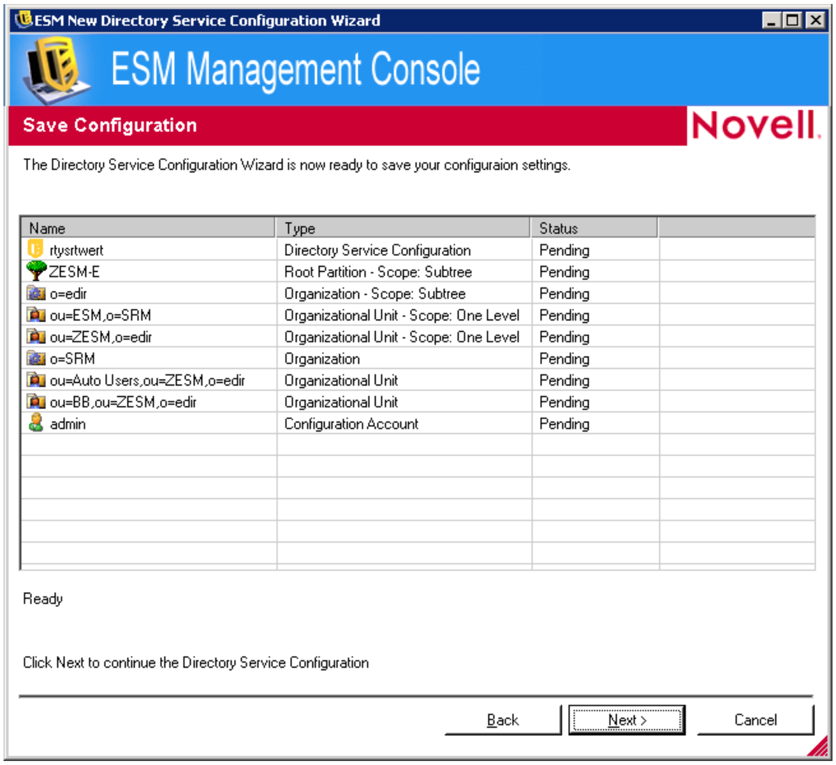
14 (Optional) Select the contexts to synchronize as part of the configuration process.

The synchronization is performed in the background so you can immediately begin using your new configuration. If you have many users and computers to synchronize, this might take a few hours.

If you do not specify contexts to synchronize, the users and computers in those contexts are populated in the Management Console when they check in.

Synchronizing contexts pre-populates the Management Console with those users and computers so that you can immediately perform actions such as creating security policies. When the users or computers check in to the system, those policies are pushed down and applied. By pre-populating the Management Console, you can immediately begin creating policies that are specific to individual users or computers, rather than creating a policy that applies to all users and computers in the context. If you do not synchronize the context, you must wait until those users and computers check in to the system before creating unique policies for different users or computers.

15 Click *Next* to display the Save Configuration page.



The Directory Service Configuration Wizard is now ready to save your configuraion settings.

Name	Type	Status
rtysrtwert	Directory Service Configuration	Pending
ZESM-E	Root Partition - Scope: Subtree	Pending
o=edir	Organization - Scope: Subtree	Pending
ou=ESM,o=SRM	Organizational Unit - Scope: One Level	Pending
ou=ZESM,o=edir	Organizational Unit - Scope: One Level	Pending
o=SRM	Organization	Pending
ou=Auto Users,ou=ZESM,o=edir	Organizational Unit	Pending
ou=BB,ou=ZESM,o=edir	Organizational Unit	Pending
admin	Configuration Account	Pending

Ready

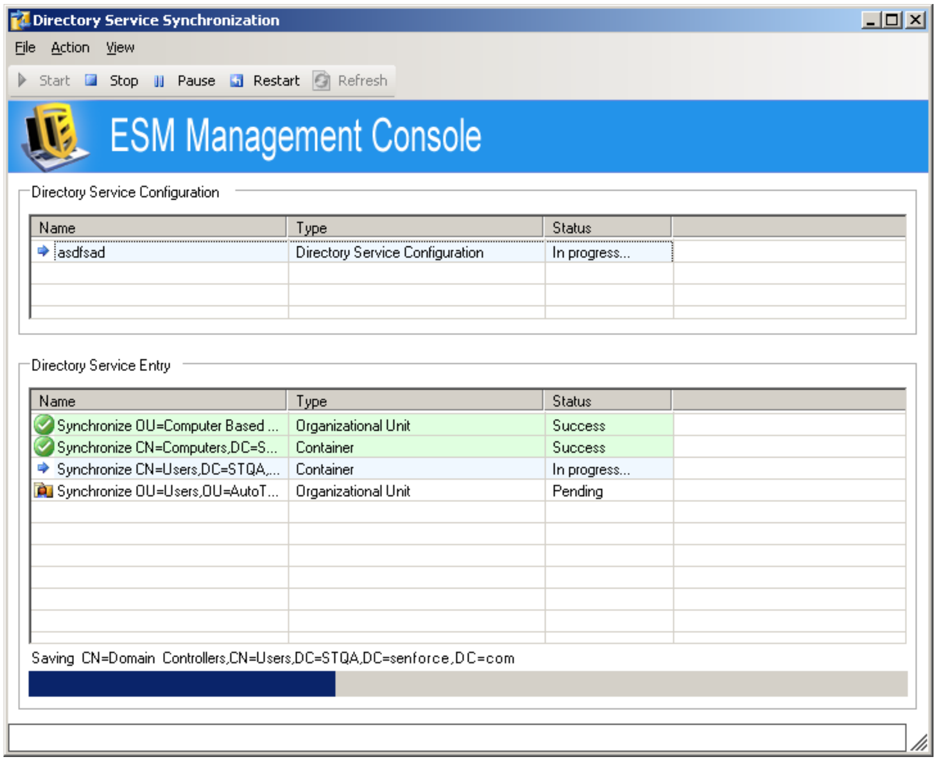
Click Next to continue the Directory Service Configuration

16 Review the information, then click *Next*.

You can click *Back* to change any settings, if necessary.

17 Click *Finish*.

When you click *Finish*, the icon displays in your Windows notification area and the synchronization begins. You can double-click the icon to display the Directory Services Synchronization dialog box.



Directory Service Configuration

Name	Type	Status
asdfsad	Directory Service Configuration	In progress...

Directory Service Entry

Name	Type	Status
✓ Synchronize OU=Computer Based ...	Organizational Unit	Success
✓ Synchronize CN=Computers,DC=S...	Container	Success
Synchronize CN=Users,DC=STQA,...	Container	In progress...
Synchronize OU=Users,OU=AutoT...	Organizational Unit	Pending

Saving CN=Domain Controllers,CN=Users,DC=STQA,DC=senforce,DC=com

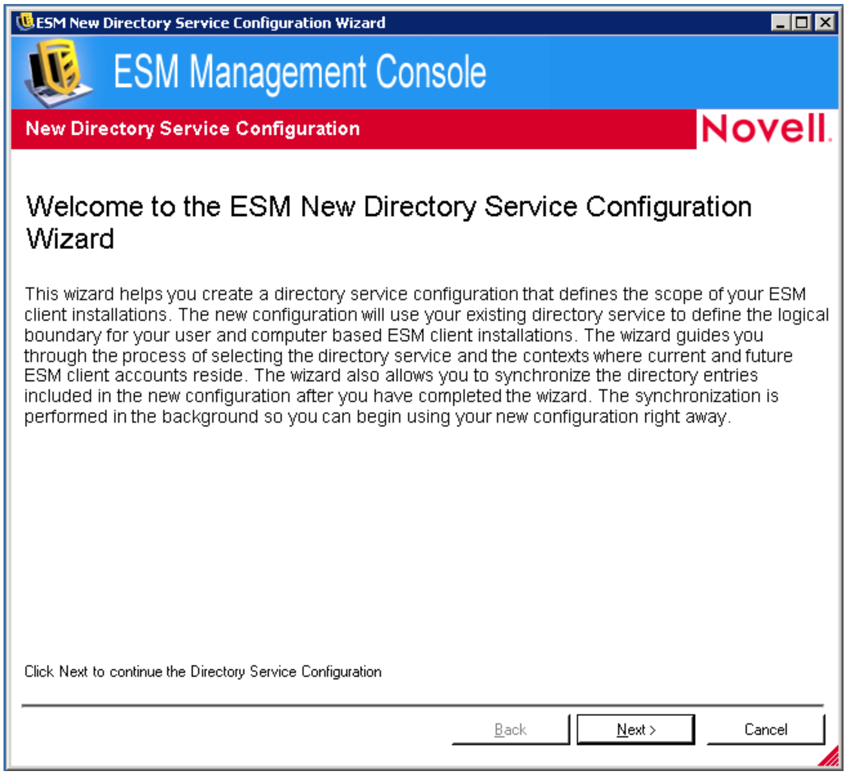
The synchronization occurs in the background. If you exit the Management Console, the synchronization stops. When you open the Management Console again, the synchronization resumes where it left off.

3.2 Configuring the Directory Service for Microsoft Active Directory

After installing ZENworks Endpoint Security Management, the New Directory Service Configuration Wizard automatically displays. If you have just installed the product and the Welcome page is displayed, skip to Step 4 in the following procedure.

To configure the directory service:

1. In the Management Console, click *Tools* > *Configuration*.
2. Click *Authenticating Directories*.
3. Click *New* to launch the New Directory Service Configuration Wizard.



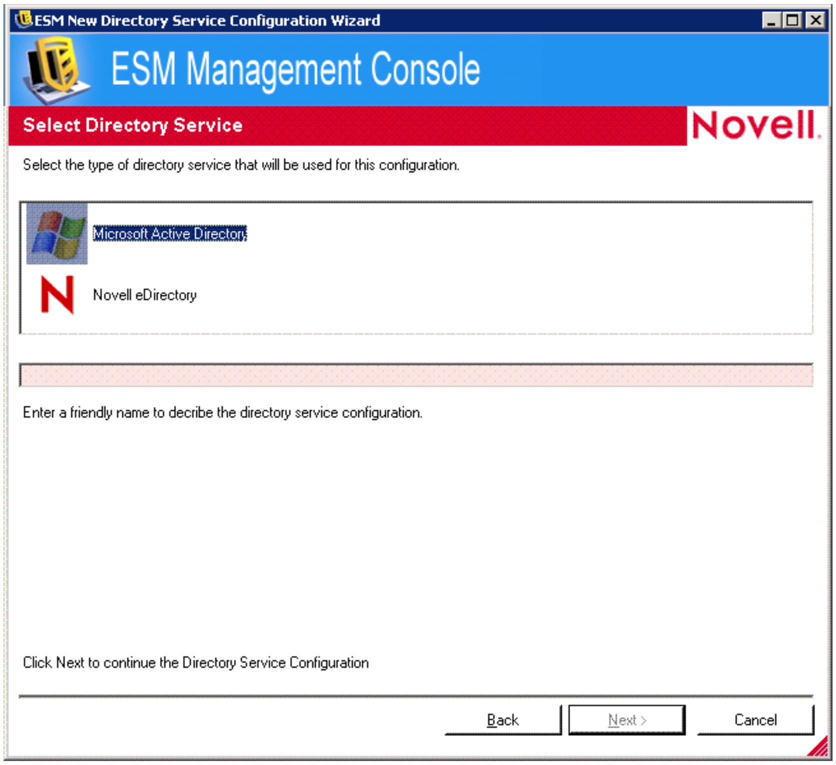
ESM New Directory Service Configuration Wizard
ESM Management Console
New Directory Service Configuration
Novell.

Welcome to the ESM New Directory Service Configuration Wizard

This wizard helps you create a directory service configuration that defines the scope of your ESM client installations. The new configuration will use your existing directory service to define the logical boundary for your user and computer based ESM client installations. The wizard guides you through the process of selecting the directory service and the contexts where current and future ESM client accounts reside. The wizard also allows you to synchronize the directory entries included in the new configuration after you have completed the wizard. The synchronization is performed in the background so you can begin using your new configuration right away.

Click Next to continue the Directory Service Configuration

4 Click *Next* to display the Select Directory Service page.



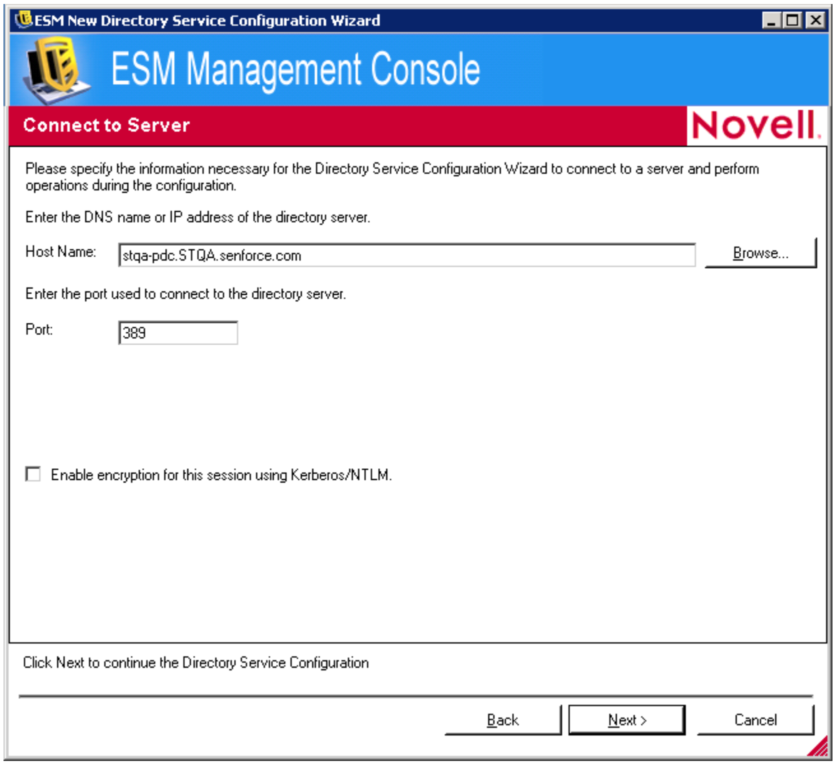
Select the type of directory service that will be used for this configuration.

Enter a friendly name to decribe the directory service configuration.

Click Next to continue the Directory Service Configuration

5 Select *Microsoft Active Directory* as the directory service.

6 Specify a friendly name to describe the directory service configuration, then click *Next* to display the Connect to Server page.



Please specify the information necessary for the Directory Service Configuration Wizard to connect to a server and perform operations during the configuration.

Enter the DNS name or IP address of the directory server.

Host Name: stqa-pdc.STQA.senforce.com

Enter the port used to connect to the directory server.

Port: 389

□ Enable encryption for this session using Kerberos/NTLM.

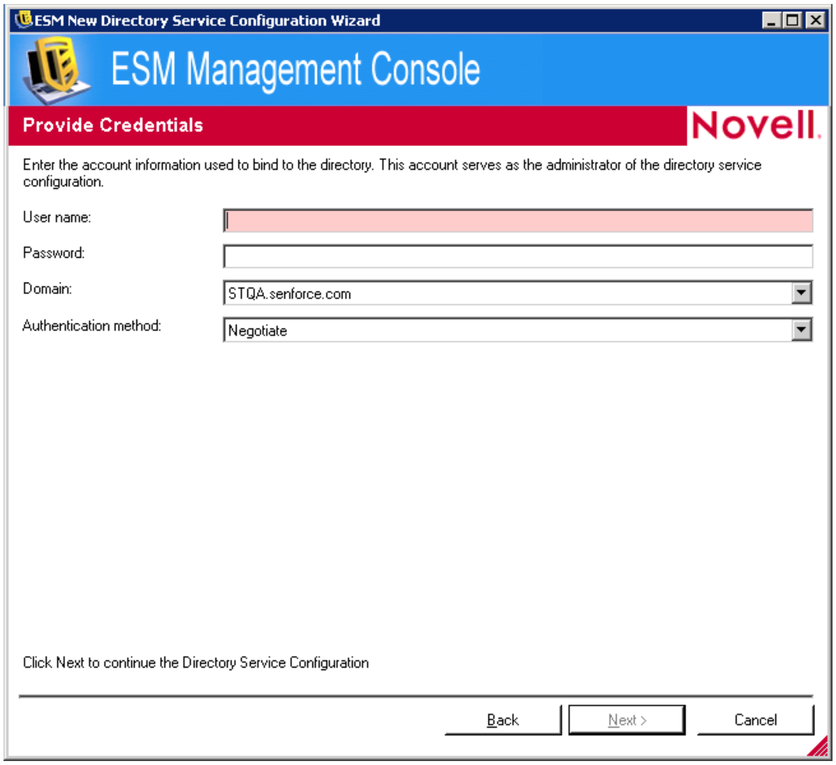
Click Next to continue the Directory Service Configuration

7 Fill in the fields:

- **Host Name:** Specify the DNS name or IP address of the directory server. If the DNS name or IP address cannot be authenticated, a bind error message displays.
- **Port:** Specify the port used to connect to the directory server.

  Port 389 is the default. If you use a different port to connect to the directory server, you can specify that port.
- **Enable Encryption for this Session using Kerberos/NTLM:** Select to enable encryption.

8 Click *Next* to display the Provide Credentials page.



Provide Credentials

Enter the account information used to bind to the directory. This account serves as the administrator of the directory service configuration.

User name:

Password:

Domain: STQA.senforce.com

Authentication method: Negotiate

Click Next to continue the Directory Service Configuration

9 Fill in the fields:

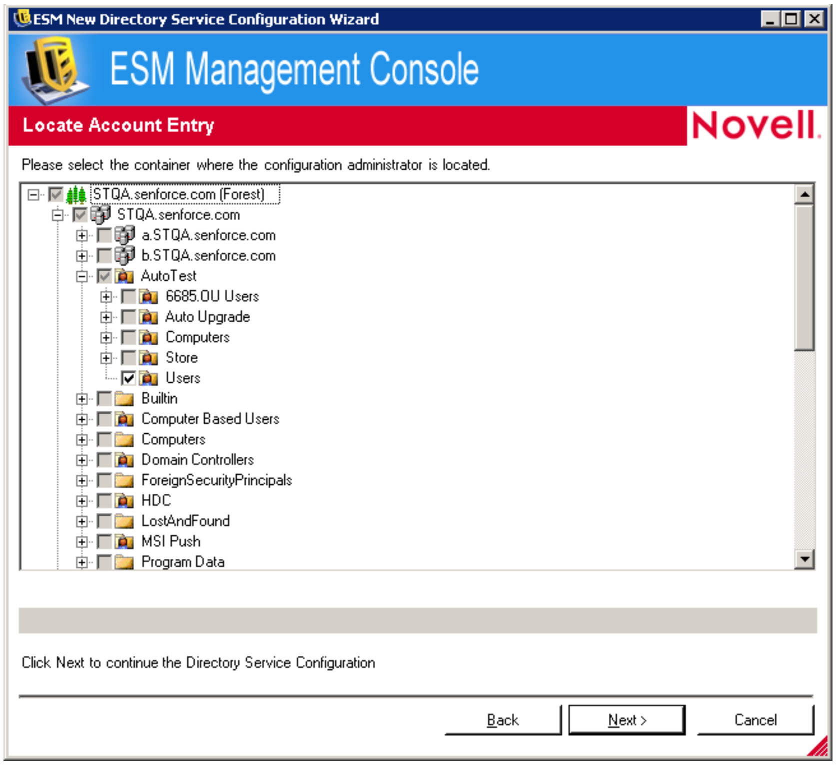
- **User name:** Specify the account administrator to bind to the directory.

  This account serves as the administrator of the directory service configuration. The login name must be a user who has permission to view the entire directory tree. It is recommended that this user be the domain administrator.
- **Password:** Specify the password for the account administrator.

  This account serves as the administrator of this directory service configuration.

  The password should not be set to expire, and this account should never be disabled.
- **Domain:** Specify the domain in which the account administrator is a member.
- **Authentication Method:** Select an authentication method:
  - Negotiate
  - Kerberos
  - NTLM

10 If the configuration administrator user you specified in Step 9 cannot be found in the domain, the Locate Account Entry page displays.



Locate Account Entry

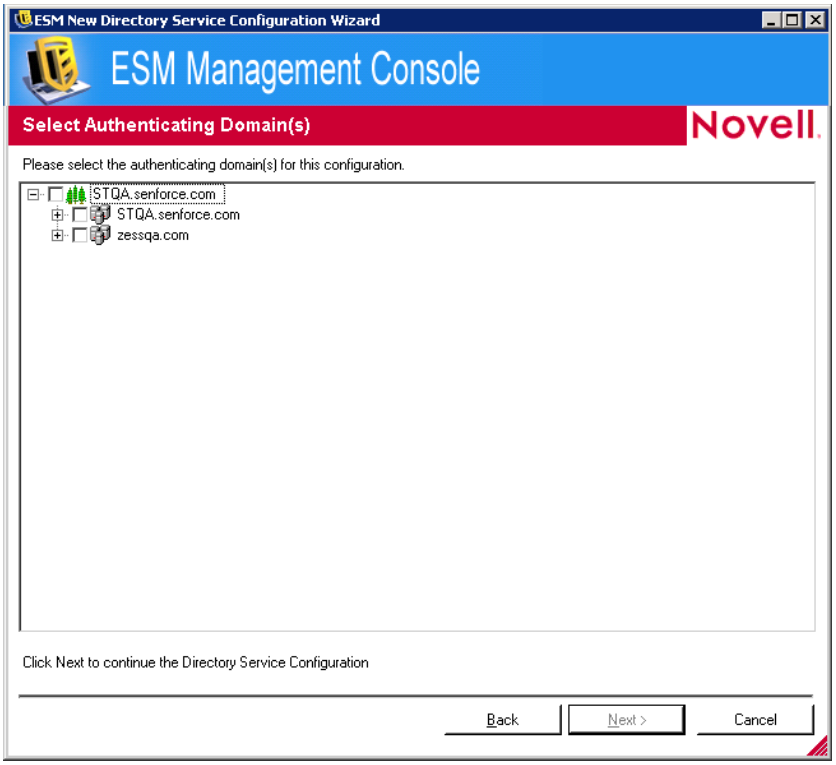
Please select the container where the configuration administrator is located.

- ☑ STQA.senforce.com (Forest)
  - ☑ STQA.senforce.com
    - □ a.STQA.senforce.com
    - □ b.STQA.senforce.com
    - ☑ AutoTest
      - □ 6685.OU Users
      - □ Auto Upgrade
      - □ Computers
      - □ Store
      - ☑ Users
    - □ Builtin
    - □ Computer Based Users
    - □ Computers
    - □ Domain Controllers
    - □ ForeignSecurityPrincipals
    - □ HDC
    - □ LostAndFound
    - □ MSI Push
    - □ Program Data

Click Next to continue the Directory Service Configuration

Specify the container where the administrator is located.

11 Click *Next* to display the Select Authenticating Domain(s) page.



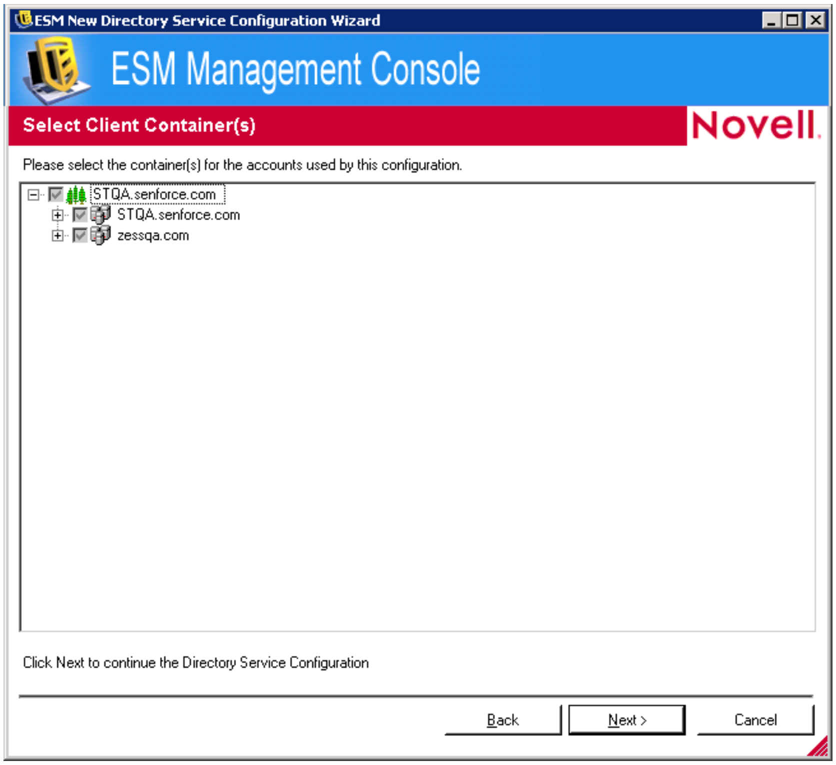
Select Authenticating Domain(s)

Please select the authenticating domain(s) for this configuration.

- □ STQA.senforce.com
  - □ STQA.senforce.com
  - □ zessqa.com

Click Next to continue the Directory Service Configuration

12 Browse to and select the authenticating domains for this configuration, then click *Next* to display the Select Client Container(s) page.



Select Client Container(s)

Please select the container(s) for the accounts used by this configuration.

☑ STQA.senforce.com
☑ STQA.senforce.com
☑ zessqa.com

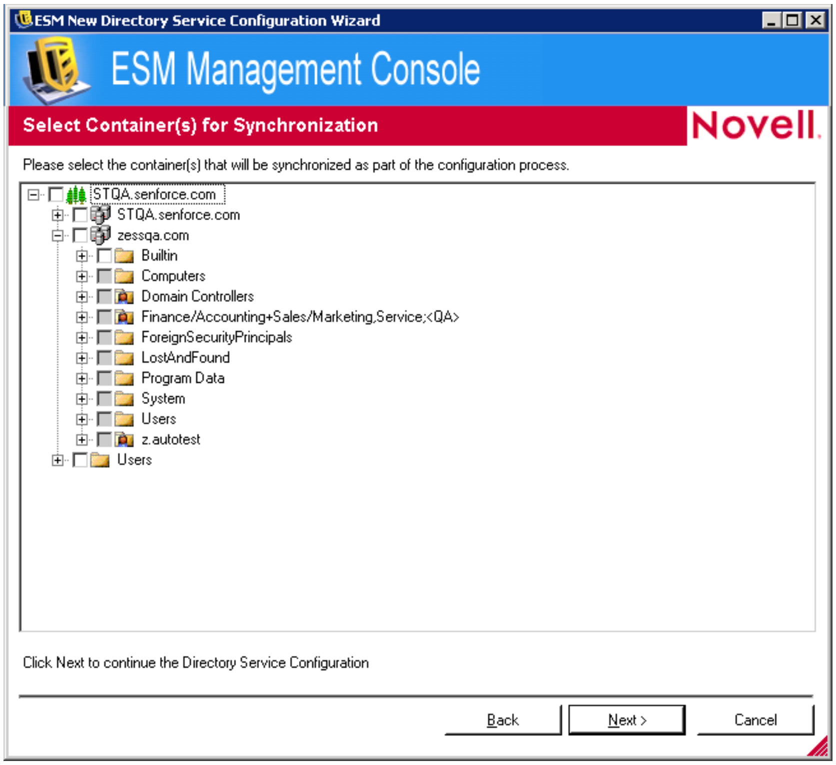
Click Next to continue the Directory Service Configuration

13 Browse to and select the containers for the accounts used in this configuration.

The Select Client Container(s) page lets you narrow the search to only those containers that contain managed users and computers, which improves performance.

Any client installation that attempts to check in with the management server the does not reside in a selected container results in longer search times.

14 Click *Next* to display the Select Container(s) for Synchronization page.



Select Container(s) for Synchronization

Please select the container(s) that will be synchronized as part of the configuration process.

```
□ STQA.senforce.com
    □ STQA.senforce.com
    □ zessqa.com
        □ Builtin
        □ Computers
        □ Domain Controllers
        □ Finance/Accounting+Sales/Marketing,Service;<QA>
        □ ForeignSecurityPrincipals
        □ LostAndFound
        □ Program Data
        □ System
        □ Users
        □ z.autotest
    □ Users
```

Click Next to continue the Directory Service Configuration

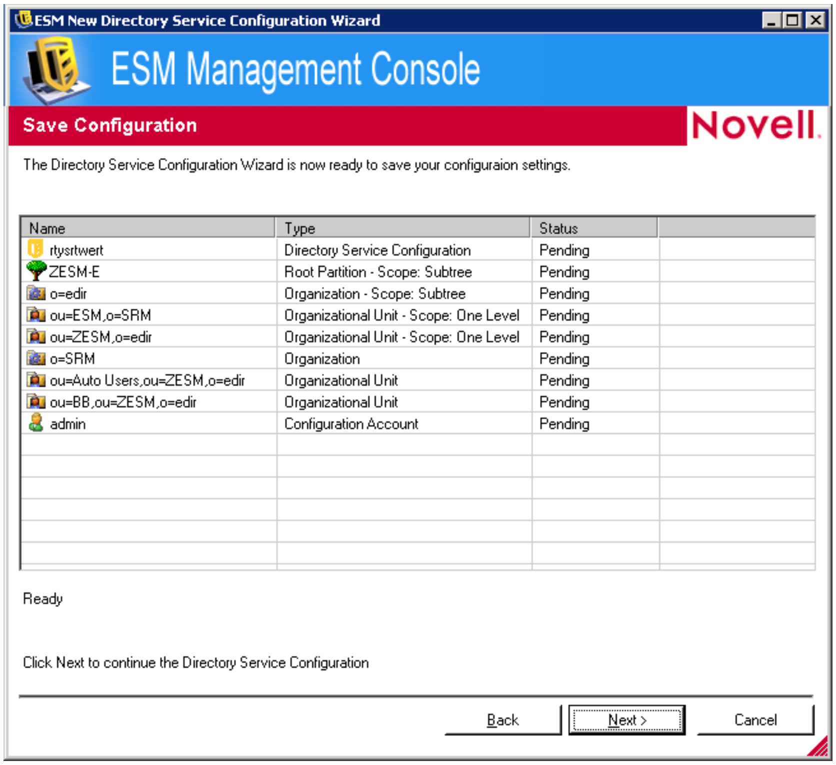
15 (Optional) Select the containers to synchronize as part of the configuration process.

The synchronization is performed in the background so you can immediately begin using your new configuration. If you have many users and computers to synchronize, this might take a few hours.

If you do not specify containers to synchronize, the users and computers in those contexts are populated in the Management Console when they check in.

Synchronizing contexts pre-populates the Management Console with those users and computers so that you can immediately perform actions such as creating security policies. When the users or computers check in to the system, those policies are pushed down and applied. By pre-populating the Management Console, you can immediately begin creating policies that are specific to individual users or computers, rather than creating a policy that applies to all users and computers in the context. If you do not synchronize the context, you must wait until those users and computers check in to the system before creating unique policies for different users or computers.

16 Click *Next* to display the Save Configuration page.



The Directory Service Configuration Wizard is now ready to save your configuraion settings.

Name	Type	Status
rtysrtwert	Directory Service Configuration	Pending
ZESM-E	Root Partition - Scope: Subtree	Pending
o=edir	Organization - Scope: Subtree	Pending
ou=ESM,o=SRM	Organizational Unit - Scope: One Level	Pending
ou=ZESM,o=edir	Organizational Unit - Scope: One Level	Pending
o=SRM	Organization	Pending
ou=Auto Users,ou=ZESM,o=edir	Organizational Unit	Pending
ou=BB,ou=ZESM,o=edir	Organizational Unit	Pending
admin	Configuration Account	Pending

Ready

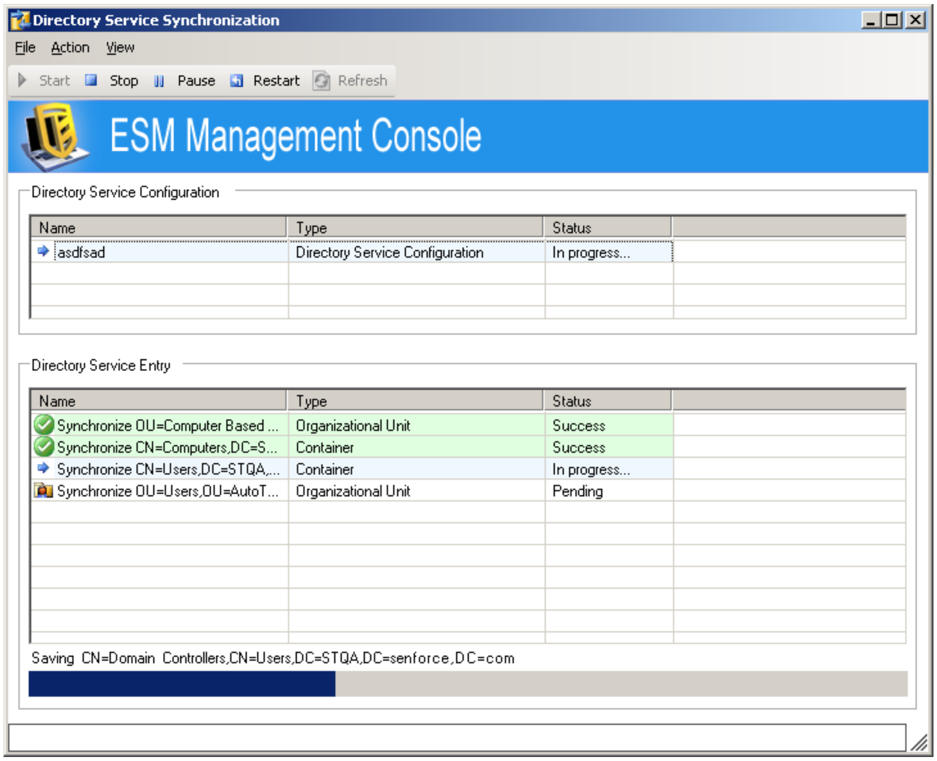
Click Next to continue the Directory Service Configuration

17 Review the information, then click *Next*.

You can click *Back* to change any settings, if necessary.

18 Click *Finish*.

When you click *Finish*, the icon displays in your Windows notification area and the synchronization begins. You can double-click the icon to display the Directory Services Synchronization dialog box.


Directory Service Synchronization
File Action View
Start Stop Pause Restart Refresh
ESM Management Console

Directory Service Configuration

Name	Type	Status
➔ asdfsad	Directory Service Configuration	In progress...

Directory Service Entry

Name	Type	Status
✓ Synchronize OU=Computer Based ...	Organizational Unit	Success
✓ Synchronize CN=Computers,DC=S...	Container	Success
➔ Synchronize CN=Users,DC=STQA,...	Container	In progress...
Synchronize OU=Users,OU=AutoT...	Organizational Unit	Pending

Saving CN=Domain Controllers,CN=Users,DC=STQA,DC=senforce,DC=com

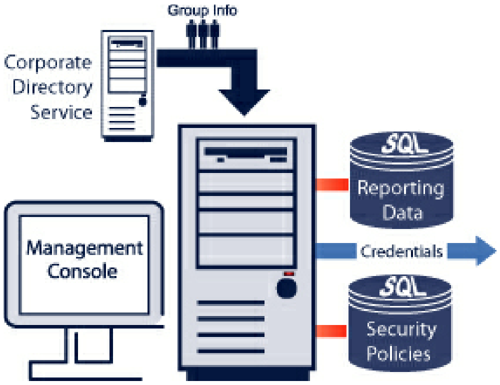
The synchronization occurs in the background. If you exit the Management Console, the synchronization stops. When you open the Management Console again, the synchronization resumes where it left off.

Using the ZENworks Endpoint Security Management Service

4

The Management Service in Novell® ZENworks® Endpoint Security Management is the central service for Endpoint Security Management. It is used to create authentication credentials, design and store security policies and their components, and provide remediation through a robust reporting service. It provides security policies and user information to the Policy Distribution Service, as well as providing opaque credentials to Endpoint Security Clients.

The following graphic illustrates the role of the Management Service:



Security policies, credentials, and reports are stored in an SQL database(s), which may reside on the same server as the Management Service or on remote servers.

The following sections contain additional information:

- Section 4.1, "About the Management Service," on page 37
- Section 4.2, "Securing Server Access," on page 38
- Section 4.3, "Distributing and Renewing ZENworks Endpoint Security Management Credentials," on page 39

4.1 About the Management Service

The following sections contain additional information:

- Section 4.1.1, "Server Selection and Installation," on page 37
- Section 4.1.2, "Server Maintenance," on page 38
- Section 4.1.3, "Upgrading the Software," on page 38
- Section 4.1.4, "Uninstall," on page 38

4.1.1 Server Selection and Installation

See *ZENworks Endpoint Security Management Installation Guide* for selection and installation instructions.

4.1.2 Server Maintenance

It is recommended that regular disk cleanup tasks be configured to run on this server to remove temporary files out of the `Windows\temp` folder. Under extreme load conditions, Windows can generate an inordinate amount of temporary files that needlessly consume disk space.

4.1.3 Upgrading the Software

To upgrade your software from one release to another, you must uninstall the old release and install the new release. Complete instructions are provided in "Upgrading" in the *ZENworks Endpoint Security Management Installation Guide*.

4.1.4 Uninstall

To uninstall the Management Service, use the Add/Remove Programs function in the Windows Control Panel.

To uninstall the Management Console (when run on a separate computer), use the Add/Remove Programs function in the Windows Control Panel.

4.2 Securing Server Access

The following sections contain information to help you secure access to your ZENworks Endpoint Security Management server:

- Section 4.2.1, "Physical Access Control," on page 38
- Section 4.2.2, "Network Access Control," on page 39
- Section 4.2.3, "High Availability," on page 39
- Section 4.2.4, "Running the Service," on page 39

4.2.1 Physical Access Control

Physical access to the Management Server should be controlled to prevent access by unauthorized parties. Measures taken should be appropriate to the risks involved. There are multiple available standards and guidelines available, including NIST recommendations, HIPAA requirements, ISO/ IEC 17799, and less formal collections of recommendations such as CISSP or SANS guidelines. Even when a given regulatory frameworks is not applicable, it may still act as a valuable resource and planning guide.

Disaster Recovery and Business Continuity mechanisms to protect the Management Server should be put in place to protect the server if an organizational risk assessment identifies a need for such steps. The mechanisms best used will depend on the specifics of the organization and its desired risk profile, and cannot be described in advance. There are multiple available standards and guidelines available, including NIST recommendations, HIPAA requirements, ISO/IEC 17799, and less formal collections of recommendations such as CISSP or SANS guidelines.

4.2.2 Network Access Control

The Management Server can be further protected from unauthorized access by restricting network access to it. This may take the form of some or all of the following:

- Restricting incoming connection attempts to those IP addresses from which a valid access attempt might be expected
- Restricting incoming connection attempts to those ports and protocols from which a valid access attempt might be expected
- Restricting outgoing connection attempts to those IP addresses to which a valid access attempt might be expected
- Restricting outgoing connection attempts to those ports and protocols to which a valid access attempt might be expected.

Such measures can be imposed through the use of standard firewall technology.

4.2.3 High Availability

High Availability mechanisms for the Management Server should be put in place if an organizational risk assessment identifies a need for such steps. There are multiple alternative mechanisms for building high availability solutions, ranging from the general (DNS round-robining, layer 3 switches, etc.) to the vendor specific (the Microsoft web site has multiple resources on high availability web services). Those implementing and maintaining an Endpoint Security Management solution should determine which class of high availability solution is most appropriate for their context. Note that the Management Server has been architected to function in non-high-availability situations, and does not require High Availability to provide its services.

4.2.4 Running 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 Section 5.3.1, “Infrastructure and Scheduling,” on page 44 for more details.

4.3 Distributing and Renewing ZENworks Endpoint Security Management Credentials

The following sections contain additional information:

- Section 4.3.1, “Distributing Endpoint Security Management Credentials (Key Management Key),” on page 39
- Section 4.3.2, “Periodic Renewal of the Key Management Key (KMK),” on page 40

4.3.1 Distributing Endpoint Security Management Credentials (Key Management Key)

The Management Service automatically distributes credentials to each Endpoint Security Client when it is installed and checks in to the Management Service for the first time. After this credential is distributed, the Endpoint Security Client is permitted to receive policies from the Policy Distribution Service, and provide reporting data to the Reporting Service.

4.3.2 Periodic Renewal of the Key Management Key (KMK)

Cryptographic best practices dictate that the KMK be renewed at regular intervals to prevent certain cryptographic attacks from being practical. This need only take place on a relatively long cycle: typically on the order of once every year, and should not be done too frequently because the change-over does involve some effort and bandwidth costs.

To renew the KMK, perform the following steps:

1. Open the Communications Console on the Management Service (*Start/Programs/Novell/Management Service/Endpoint Security Management Communications Console*).

   NOTE: Running the Communications Console causes the Management Service to lose user and log data; however, policy data is not deleted.

2. Allow the Communications Console to run a complete check.
3. Have all end users authenticate to the Management Service (either via VPN or while inside the appropriate firewall), by right-clicking the Endpoint Security Client taskbar icon, then clicking *Check for Policy Update*.
4. The Management Console automatically passes the new KMK credentials down. In some cases, the user must authenticate to the domain (username and password).

Until the endpoints renew their KMK, they will not be able to communicate with the Policy Distribution Service.

Using the ZENworks Storage Encryption Solution Management Console

5

The Management Console in Novell® ZENworks® Endpoint Security Management is the central access and control mechanism for the Management Service.

Double-click the ESM Management Console icon on the desktop to launch the login window. Log in to the console by entering the administrator name and password. The username entered must be an authorized user on the Management Service.

NOTE: It is recommended that the console be closed or minimized when not in use.

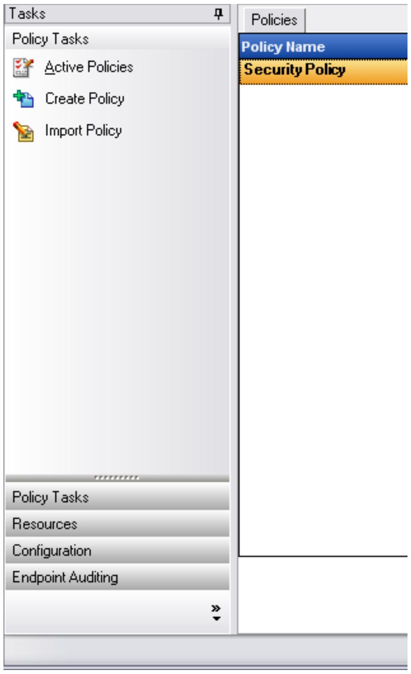
The following sections contain additional information:

- Section 5.1, "Using the Console Taskbar," on page 41
- Section 5.2, "Using the Console Menu Bar," on page 43
- Section 5.3, "Using the Configuration Window," on page 44
- Section 5.4, "Using Alerts Monitoring," on page 47
- Section 5.5, "Using Reports," on page 51
- Section 5.6, "Generating Custom Reports," on page 60
- Section 5.7, "Using the ZENworks Storage Encryption Solution," on page 71
- Section 5.8, "Managing Keys," on page 72

5.1 Using the Console Taskbar

The taskbar on the left provides access to the Management Console tasks. If the taskbar is not visible, click the *Tasks* button.

Figure 5-1 The Management Console



The functions available in the taskbar are described in the following sections:

- Section 5.1.1, "Policy Tasks," on page 42
- Section 5.1.2, "Resources," on page 43
- Section 5.1.3, "Configuration," on page 43
- Section 5.1.4, "Endpoint Auditing," on page 43

5.1.1 Policy Tasks

The primary function of the Management Console is the creation and dissemination of security policies. The Policy Tasks guide the administrator through creating and editing security policies that are used by the Endpoint Security Client to apply centrally managed security to each endpoint.

The Policy Tasks include the following:

- **Active Policies:** Displays a list of current policies, which can be reviewed and edited. Click the policy to open it.
- **Create Policy:** Starts the policy creation process. For more information, see Chapter 6, "Creating and Distributing Security Policies," on page 75.
- **Import Policy:** Imports policies created using other management services. For more information, see Section 6.4.1, "Importing Policies," on page 169.

Clicking any of the policy tasks minimizes the taskbar. Click the Tasks button left side of the Management Console to display it again.

5.1.2 Resources

The following resources are available to help you:

- **Contact Support:** Launches a browser to display the Novell Contacts and Offices page.
- **Online Technical Help:** Launches a browser to display the Novell Training and Support page.
- **Management Console Help:** Launches Help.

5.1.3 Configuration

The Management Service Configuration tasks provide controls for both the ZENworks Endpoint Security Management server infrastructure and controls for monitoring additional enterprise directory services. See Section 5.3, "Using the Configuration Window," on page 44 for details. This control is not available when running a "Stand-Alone" Management Console. See the *ZENworks Endpoint Security Management Installation Guide* for more information.

5.1.4 Endpoint Auditing

Endpoint Auditing gives you access to Endpoint Security Management Reporting and Alerting.

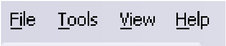
Alerts monitoring ensures that any attempts to compromise corporate security policies are reported in the Management Console. This allows the ZENworks Endpoint Security Management administrator to know of potential problems and take any appropriate remedial actions. The Alerts dashboard is completely configurable, granting total control over when and how frequently alerts are triggered. See Section 5.4, "Using Alerts Monitoring," on page 47 for details.

Reporting is critical in assessing and implementing strong security policies. Reports can be accessed through the Management Console by clicking *Reporting*. The endpoint security information gathered and reported back is also completely configurable, and can be gathered by domain, group, or individual user. See Section 5.5, "Using Reports," on page 51 for details.

5.2 Using the Console Menu Bar

The menu bar gives you access to all functions of the Management Console. As with all Windows menus, simply click the menu link to display the menu items. The menu items are described below.

Figure 5-2 *Menu Bar*



- **File:** Lets you create and manage policies.
  - **Create New Policy:** Starts the process to create a new policy.
  - **Refresh Policy List:** Updates the list to display all active policies.
  - **Delete Policy:** Deletes the selected policy.
  - **Import Policy:** Imports a policy into the Management Console.
  - **Export Policy:** Exports a policy and the required `setup.sen` file to a specified location outside of the Management Service database.
  - **Exit:** Closes the Management Console software, logging out the user.

- **Tools:** Lets you control the Management Service.
  - **Configuration:** Opens the Configuration window.
  - **Export Encryption Keys:** Displays the Export Encryption Keys(s) dialog box.
  - **Import Encryption Keys:** Displays the Import Encryption Keys(s) dialog box.
  - **Generate New Key:** Creates and activates a new encryption key for policies enforcing data protection.
- **View:** Lets you change access key policy tasks without using the taskbar.
  - **Active Policies:** When a policy is open, switches the view to that policy.
  - **Alerts:** Displays the *Alerts* dashboard.
  - **Reporting:** Displays the *Reporting* dashboard.
- **Help:** Lets you access to the Management Console Help and the About box.
  - **Help:** Launches the Management Console Help tool, which guides you through policy creation as well as all Management Console tasks (also available by pressing the F1 key on your keyboard).
  - **About:** Launches the About window, which displays the installation type (ESM or UWS (see Section 1.4, “USB/Wireless Security,” on page 14) and the current version number for the Management Console. This window is also where the license key is entered if you purchase the product after installation.

5.3 Using the Configuration Window

The Configuration window gives the ZENworks Endpoint Security Management administrator access to the Infrastructure and Scheduling, Authenticating Directories, and Server Synchronization controls.

NOTE: This function is not available if this is a Stand-Alone Management Console.

To access the Configuration window:

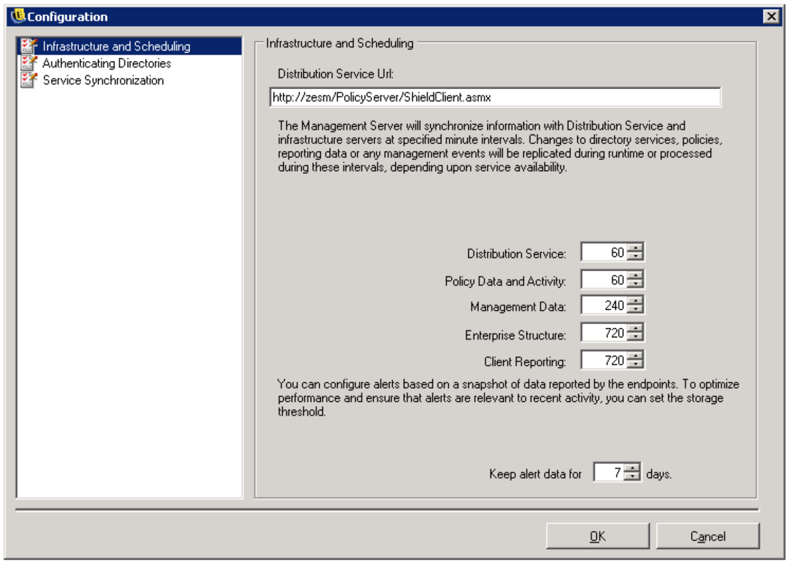
1. Click *Tools* > *Configuration*.
2. Click one of the following options in the left pane:

- Section 5.3.1, “Infrastructure and Scheduling,” on page 44
- Section 5.3.2, “Authenticating Directories,” on page 46
- Section 5.3.3, “Service Synchronization,” on page 47

5.3.1 Infrastructure and Scheduling

The Infrastructure and Scheduling module allows the ZENworks Endpoint Security Management administrator to designate and change the Policy Distribution Service URL and control the synchronization intervals for the ZENworks Endpoint Security Management components.

Figure 5-3 *Infrastructure and Scheduling Window*


Configuration
Infrastructure and Scheduling
Authenticating Directories
Service Synchronization
Infrastructure and Scheduling
OK
Cancel

Distribution Service Url: http://zesm/PolicyServer/ShieldClient.asmx

The Management Server will synchronize information with Distribution Service and infrastructure servers at specified minute intervals. Changes to directory services, policies, reporting data or any management events will be replicated during runtime or processed during these intervals, depending upon service availability.

Distribution Service: 60

Policy Data and Activity: 60

Management Data: 240

Enterprise Structure: 720

Client Reporting: 720

You can configure alerts based on a snapshot of data reported by the endpoints. To optimize performance and ensure that alerts are relevant to recent activity, you can set the storage threshold.

Keep alert data for 7 days.

The following sections contain more information about the Infastructure and Scheduling options:

- "Distribution Service URL" on page 45
- "Scheduling" on page 45

Distribution Service URL

Use this option to update the Policy Distribution Service location for both the Management Service and all Endpoint Security Clients (without requiring them to be reinstalled) if the Policy Distribution Service is moved to a new server. The URL for the current server is listed in the text field. Only the server name should be changed to point to the new server. Do not change any information after the server name.

Example:

NOTE: If the current URL is listed as `http:\\ACME\PolicyServer\ShieldClient.asmx` and the Policy Distribution Service has been installed on a new server, ACME 43, the URL should be updated as follows: `http:\\ACME43\PolicyServer\ShieldClient.asmx`.

After the URL has been updated, click *OK* to update all policies and send an automatic update of the Policy Distribution Service. This also updates the Management Service.

When changing the server URL, it is recommended that the old Policy Distribution Service not be terminated until the updated policies have a 100 percent adherence level. For more information, see Section 5.5, "Using Reports," on page 51).

Scheduling

The Scheduling components permit the ZENworks Endpoint Security Management administrator to designate when the Management Service will synchronize with other ZENworks Endpoint Security Management components, to ensure that all data and queued jobs match any recent activity, and to schedule the SQL maintenance jobs. All time increments are listed in minutes.

The following scheduling options are available:

- **Distribution Service:** Sets the synchronization schedule with the Policy Distribution Service.
- **Policy Data and Activity:** Sets the synchronization schedule with policy updates.
- **Management Data:** Sets the policy synchronization with the Management Service.
- **Enterprise Structure:** Sets the synchronization schedule with the enterprise directory service (eDirectory, Active Directory, NT Domain, and LDAP). Changes in the enterprise directory service are monitored so that corresponding changes in user-policy assignments are detected and sent to the Policy Distribution Service for Client authentication.
- **Client Reporting:** Sets the frequency that the Management Service interrogates for and downloads reporting data from the Policy Distribution Service.
- **Keep Alert Data for *x* Days:** Configures alerts based on a snapshot of data reported by the endpoints. To optimize performance, and to ensure that alerts are relevant to recent activity, you can se the storage threshold based on a number of days.

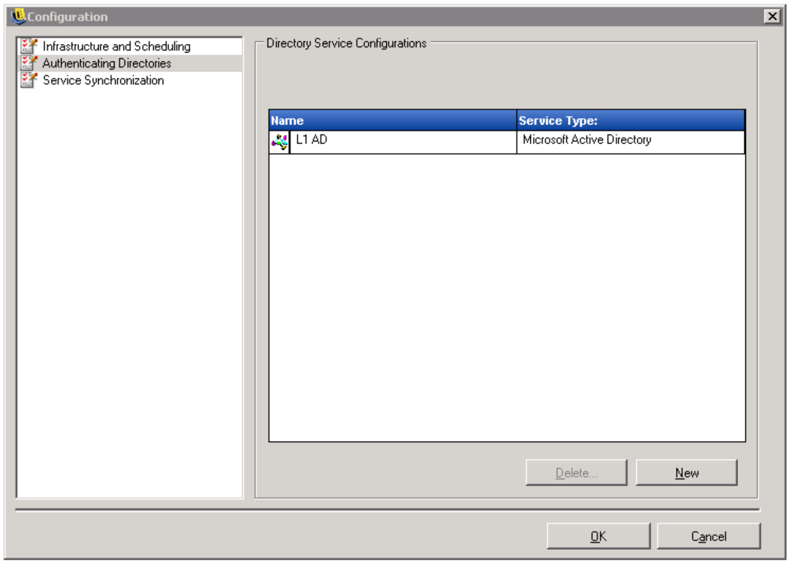
5.3.2 Authenticating Directories

Policies are distributed to end users by interrogating the Enterprise's existing directory service (eDirectory, Active Directory, and NT Domains). The Authenticating Directories service is responsible for handling end-user credentials and authentication issues for the Policy Distribution Service.

NT Domain is supported only when the Management Service is installed on a Windows 2000 or Windows 2000 advanced server (SP4).

An initial directory service is normally detected and monitored during the Management Service communication check at installation. Authenticating Directories can, if required, manage users from multiple directories and multiple directory platforms.

Figure 5-4 *Authenticating Directories Window*


Configuration
Infrastructure and Scheduling
Authenticating Directories
Service Synchronization
Directory Service Configurations
Delete...
New
OK
Cancel

Name	Service Type:
L1 AD	Microsoft Active Directory

All information, with the exception of the directory type may be updated.

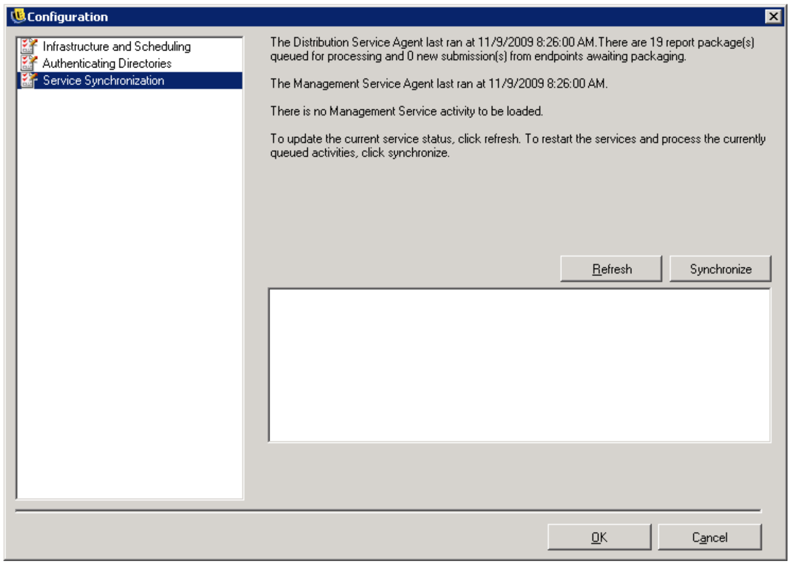
To add a new directory service:

1. Click *New* to launch the New Directory Service Configuration Wizard.
2. Follow the prompts to complete the wizard. For detailed steps to complete the wizard, see Chapter 3, "Configuring the Directory Service," on page 21.

5.3.3 Service Synchronization

The Service Synchronization control lets you to force a synchronization of the Management Service and Policy Distribution Service. This updates all alerting, reporting, and policy distribution.

Figure 5-5 *Service Synchronization*



The Distribution Service Agent last ran at 11/9/2009 8:26:00 AM.There are 19 report package(s) queued for processing and 0 new submission(s) from endpoints awaiting packaging.

The Management Service Agent last ran at 11/9/2009 8:26:00 AM.

There is no Management Service activity to be loaded.

To update the current service status, click refresh. To restart the services and process the currently queued activities, click synchronize.

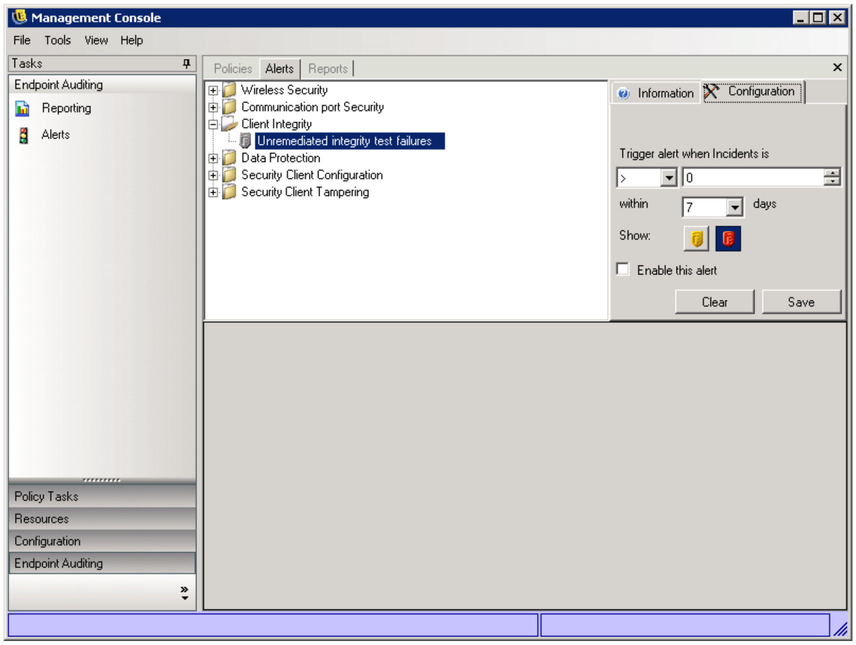
To update the current service status, click *Refresh*.

To restart the services and process the currently queued activities, click *Synchronize*.

5.4 Using Alerts Monitoring

Alerts monitoring allows the ZENworks Endpoint Security Management administrator to effortlessly gauge the security state of all ZENworks Endpoint Security Management managed endpoints throughout the enterprise. Alerts triggers are fully configurable and can report either a warning or a full emergency alert. This tool is accessed either through *Endpoint Auditing* on the taskbar or by using the *View* menu.

Figure 5-6 *Alerts Dashboard*



Trigger alert when Incidents is: > 0

within: 7 days

Show:

□ Enable this alert

Alerts monitoring is available for the following areas:

- **Client Integrity:** Notifies the administrator of unremediated integrity test results.
- **Communication Port Security:** Notifies the administrator of potential port scan attempts.
- **Data Protection:** Notifies the administrator of files that are copied to removable storage devices within a one-day period.
- **Security Client Configuration:** Notifies the administrator of incorrect security client versions and incorrect policies.
- **Security Client Tampering:** Notifies the administrator of user hack attempts, uninstall attempts, and usage of the override password.
- **Wireless Security:** Notifies the administrator of unsecure access points, both detected and connected to by the end user.

The following sections contain additional information:

- Section 5.4.1, "Configuring Endpoint Security Management for Alerts," on page 48
- Section 5.4.2, "Configuring Alert Triggers," on page 49
- Section 5.4.3, "Managing Alerts," on page 50

5.4.1 Configuring Endpoint Security Management for Alerts

Alerts monitoring requires reporting data be collected and uploaded at regular intervals to give the most accurate picture of the current endpoint security environment. Unmanaged Endpoint Security Clients do not provide reporting data, and will therefore, not be included in the Alerts monitoring.

The following sections contain more information:

- "Activating Reporting" on page 49
- "Optimizing Synchronization" on page 49

Activating Reporting

Reporting should be activated in each security policy. See Section 6.2.4, "Compliance Reporting," on page 118 for details on setting up reporting for a security policy. Adjust report send times to an interval that will give you consistent updates on endpoint status. Additionally, an alert will not activate without a report. Any activity you want to be alerted to must have an appropriate report assigned to it in the security policy.

Optimizing Synchronization

By default, the ZENworks Endpoint Security Management Reporting Service syncs every 12 hours. This means that reporting and alerts data are not ready until 12 hours have passed from installation. To adjust this time, open the Configuration tool (see "Scheduling" on page 45) and adjust the Client Reporting time to the number of minutes appropriate for your needs and your environment.

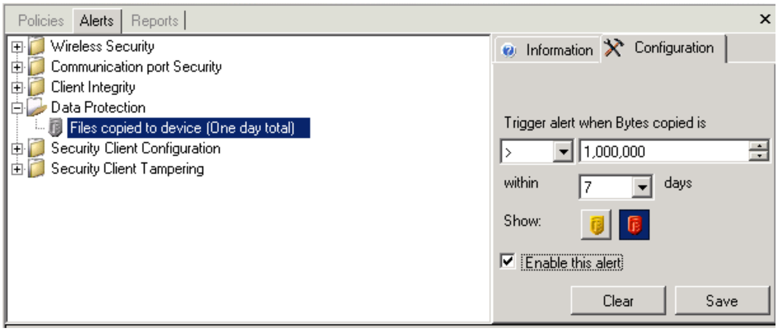
When data is needed immediately, the Service Synchronization option in the Configuration tool immediately lynches the Policy Distribution Service (which collects the reporting data from the endpoints) and the Reporting Service, which updates all alerts based on the newly collected data. See Section 5.3.3, "Service Synchronization," on page 47 for details.

5.4.2 Configuring Alert Triggers

Alert triggers can be adjusted to thresholds that fit your corporate security needs.

To adjust alerts from their defaults:

1 Select an alert from the list and click the *Configuration* tab.


Policies
Alerts
Reports
Wireless Security
Communication port Security
Client Integrity
Data Protection
Files copied to device (One day total)
Security Client Configuration
Security Client Tampering
Information
Configuration
Clear
Save

Trigger alert when Bytes copied is > 1,000,000

within 7 days

Show:

☑ Enable this alert

2 Adjust the trigger threshold by selecting the condition from the drop-down list. This states whether the trigger number is:

- Equal to (=)
- Greater than (<)
- Greater than or equal to (<=)
- Less than (>)
- Less than or equal to (>=)

3 Adjust the trigger number. This number varies, depending upon the type of alert.

4 Select the number of days that this number must be met.

5 Select the trigger type, whether it’s the warning icon (🟨) or the emergency icon (🟥).

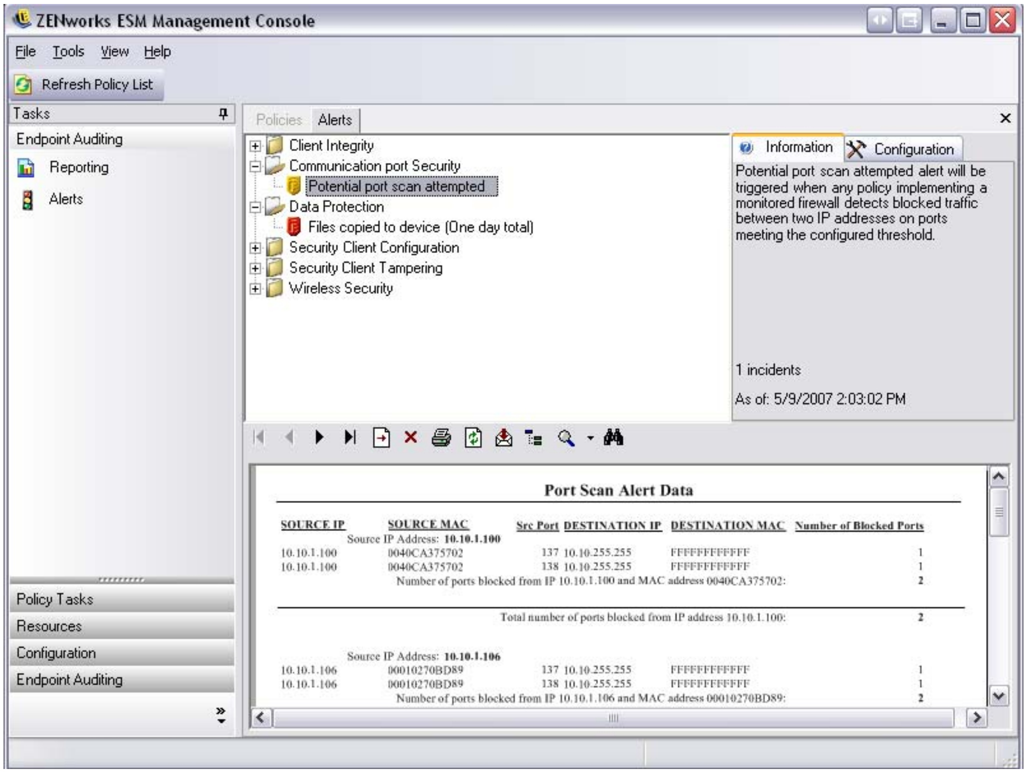
6 Click *Enable this alert*.

7 Click *Save*.

5.4.3 Managing Alerts

Alerts notify you of issues that need to be remedied within the endpoint security environment. Remediation is normally handled on a case-by-case and individual or group basis. To help identify the issue, Alert reports are displayed when the alert is selected.

Figure 5-7 *Alert Reporting*



Potential port scan attempted alert will be triggered when any policy implementing a monitored firewall detects blocked traffic between two IP addresses on ports meeting the configured threshold.

1 incidents

As of: 5/9/2007 2:03:02 PM

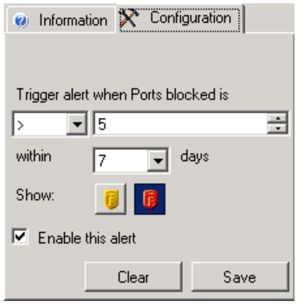
```
                                  Port Scan Alert Data

SOURCE IP       SOURCE MAC          Src Port DESTINATION IP  DESTINATION MAC  Number of Blocked Ports
           Source IP Address:  10.10.1.100
10.10.1.100     0040CA375702            137  10.10.255.255   FFFFFFFFFFFF                           1
10.10.1.100     0040CA375702            138  10.10.255.255   FFFFFFFFFFFF                           1
               Number of ports blocked from IP 10.10.1.100 and MAC address 0040CA375702:            2

                         Total number of ports blocked from IP address 10.10.1.100:                 2

           Source IP Address:  10.10.1.106
10.10.1.106     00010270BD89            137  10.10.255.255   FFFFFFFFFFFF                           1
10.10.1.106     00010270BD89            138  10.10.255.255   FFFFFFFFFFFF                           1
               Number of ports blocked from IP 10.10.1.106 and MAC address 00010270BD89:            2
```

This report displays the current trigger results, displaying information by affected user or device. The data provides the necessary information to take remediation actions to correct any potential corporate security issues. Additional information can be found by opening *Reporting*.

Once remediation actions have been taken, the alert remains active until the next reporting update.

To clear an alerts:

1 Select an alert from the list, then click the *Configuration* tab on the right.



Trigger alert when Ports blocked is

> 5

within 7 days

Show:

☑ Enable this alert

2 Click *Clear* to clear the reporting data from Alerts (this data is still available in the reporting database), and will not reactivate until new data is received.

5.5 Using Reports

The Reporting Service provides Adherence and Status reports for the enterprise. The available data is provided for directories and user groups within a directory. Novell reports provide feedback on the effects individual policy components can have on enterprise endpoints. Requests for these reports are set in the Security Policy (see Section 6.2.4, “Compliance Reporting,” on page 118) and provide useful data to determine policy updates.

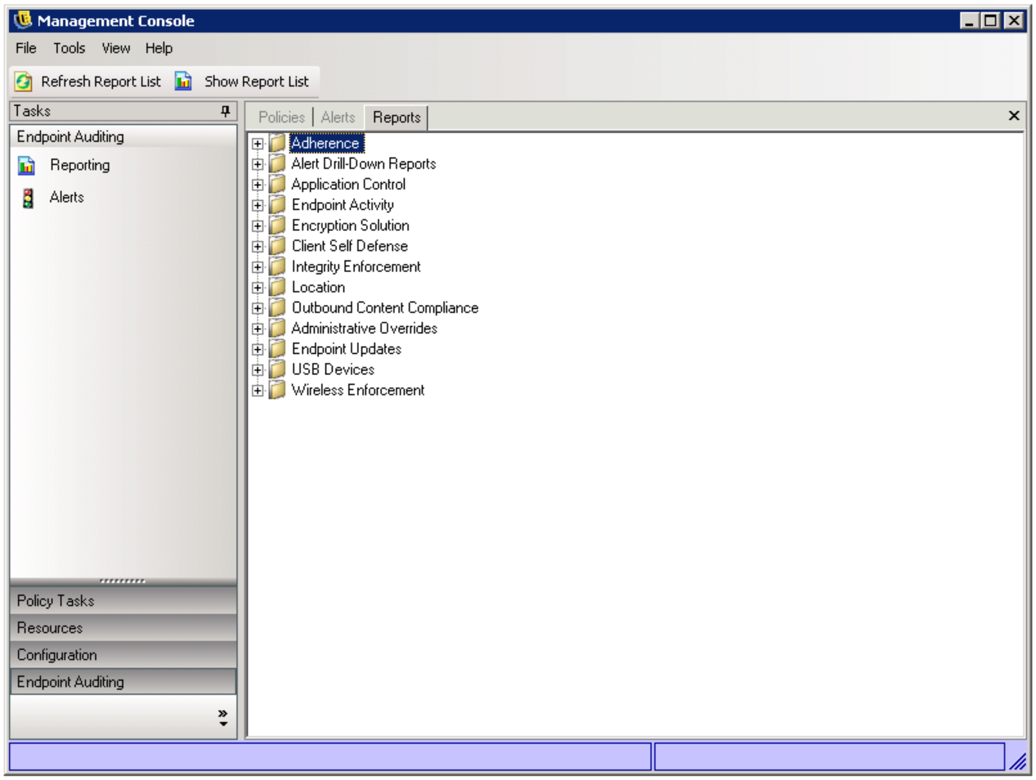
The following sections contain more information:

- Section 5.5.1, “Using the Reports Tools,” on page 51
- Section 5.5.2, “Adherence Reports,” on page 53
- Section 5.5.3, “Alert Drill-Down Reports,” on page 55
- Section 5.5.4, “Application Control Reports,” on page 56
- Section 5.5.5, “Endpoint Activity Reports,” on page 56
- Section 5.5.6, “Encryption Solutions Reports,” on page 57
- Section 5.5.7, “Client Self Defense Reports,” on page 57
- Section 5.5.8, “Integrity Enforcement Reports,” on page 57
- Section 5.5.9, “Location Reports,” on page 58
- Section 5.5.10, “Outbound Content Compliance Reports,” on page 58
- Section 5.5.11, “Administrative Overrides Reports,” on page 59
- Section 5.5.12, “Endpoint Updates Reports,” on page 59
- Section 5.5.13, “USB Devices Reports,” on page 60
- Section 5.5.14, “Wireless Enforcement Reports,” on page 60

5.5.1 Using the Reports Tools

You can select *Reporting* from either the Endpoint Auditing taskbar or from the *View* menu. The list of available reports displays (click on the "plus" sign icons next to each report type to expand the list).

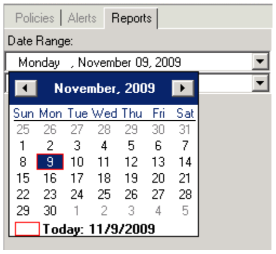
Figure 5-8 Reports Menu



- Adherence
- Alert Drill-Down Reports
- Application Control
- Endpoint Activity
- Encryption Solution
- Client Self Defense
- Integrity Enforcement
- Location
- Outbound Content Compliance
- Administrative Overrides
- Endpoint Updates
- USB Devices
- Wireless Enforcement

Reports are configured by identifying the date range and other parameters (for example, user or location). To set the dates, select the report, click *Configure*, click the date selector to expand to the calendar view, then select the month and day (be sure to click on the day to change the date parameter).

Figure 5-9 Use calendar tool to set the date-range



Date Range:

Monday , November 09, 2009

November, 2009

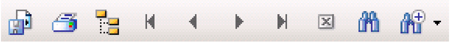
Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

Today: 11/9/2009

Click *View* to generate the report.

After a report is generated, it can be viewed through the Management Console, printed, e-mailed, or or exported as a `.pdf` file by using the Report toolbar.

Figure 5-10 Report Toolbar



When reviewing reports, the arrow buttons help you navigate through each page of the report. Reports typically have charts and graphs on the first page, with the gathered data on the remaining pages, ordered by date and type.

Use the *Printer* button to print the full report using the default printer for this computer.

Use the *Export* button to save the report as a PDF file, Excel spreadsheet, Word document, or RTF file for distribution.

Use the *Group Tree* button to toggle a list of parameters to the side of the report. Select any of these parameters to drill down farther into the report. Click the *Group Tree* button to close the sidebar.

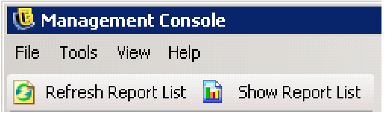
Use the *Magnifying Glass* button to display a drop-down menu to adjust the current view size.

Use the *Binoculars* button to open a search window.

When you mouse over a certain parameter, such as a user name or device name, the mouse pointer changes to a magnifying glass. You can double-click that particular item and display a new report for just that object. Click the *X* button to close the current view and return to the original report.

To return to the report list, click the *Show Report List* icon above the report window.

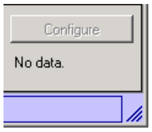
Figure 5-11 *Report list icon*



Reports are not available until data has been uploaded from the Endpoint Security Clients. By default, the ZENworks Endpoint Security Management Reporting service syncs every 12 hours. This means that reporting and alerts data will not be ready until 12 hours have passed from installation. To adjust this time frame, open the Configuration tool (see "Scheduling" on page 45), and adjust the Client Reporting time to the number of minutes appropriate for your needs and your environment.

Reports that do not have data available will have the *Configure* or *Preview* button grayed out, with the words No data underneath.

Figure 5-12 *No data*



5.5.2 Adherence Reports

Adherence Reports provide compliance information about the distribution of security policies to managed users. A score of 100 percent adherence indicates that all managed users have checked in and received the current policy.

Click the plus sign next to *Adherence* to expand the list to display the following reports:

- "Endpoint Check-In Adherence" on page 54
- "Endpoints that Never Checked-In" on page 54

- "Endpoint Client Versions" on page 54
- "Group Policy Non-Compliance" on page 54
- "Endpoint State History by Machine" on page 54
- "Policy Assignment" on page 54
- "Endpoint State History by User" on page 54

Endpoint Check-In Adherence

Provides a summary of the days since check-in by enterprise endpoints, and the age of their respective current policy. These numbers are averaged to summarize the report. This report requires no variables be entered. The report displays the users by name, which policies have been assigned to them, the days since their last check-in, and the age of the policy.

Endpoints that Never Checked-In

Lists the user accounts that have registered with the Management Service but have never checked with the Distribution Service for a policy update. Select one or more groups to generate the report.

NOTE: These may be Management Console users who don't have a Security Client installed in their names.

Endpoint Client Versions

Lists the most recently reported version of the client on each endpoint. Set the date parameters to generate this report.

Group Policy Non-Compliance

Lists groups in which some users do not have the correct policy. Selections can be made for one or more groups to generate the report.

Endpoint State History by Machine

Lists the most recent status (in a given date-range) of ZENworks Endpoint Security Management-protected endpoints, grouped by machine name. It displays the logged-on user name, current policy, ZENworks Endpoint Security Management client version, and network location. This report requires a range of dates to be entered. The administrator can drill down by double-clicking any entry to see a complete list of status reports for a particular machine.

Policy Assignment

Lists the users or groups (accounts) that have received the specified policy. Select the desired policy from the list and click *View* to run the report.

Endpoint State History by User

Lists the most recent status (in a given date-range) of ZENworks Endpoint Security Management-protected endpoints, grouped by user name. It displays the machine name, current policy, Endpoint Security Management client version, and network location. This report requires a range of dates to be entered. The administrator can drill down by double-clicking any entry to see a complete list of status reports for a particular user.

5.5.3 Alert Drill-Down Reports

Additional alert information is available in these drill-down reports. These reports only display data when an alert has been triggered. Clearing an alert also clears the alert report; however, the data is still available in a standard report.

Click the plus sign next to *Alert Drill-Down Reports* to expand the list to display the following reports:

- "Client Tampering Alert Data" on page 55
- "Files Copied Alert Data" on page 55
- "Incorrect Client Version Alert Data" on page 55
- "Incorrect Client Policy Alert Data" on page 55
- "Override Attempts Alert Data" on page 55
- "Integrity Failures Alert Data" on page 55
- "Port Scan Alert Data" on page 55
- "Uninstall Attempt Alert Data" on page 56
- "Unsecure Access Point Alert Data" on page 56
- "Unsecure Access Point Connection Alert Data" on page 56

Client Tampering Alert Data

Lists instances where a user has made an unauthorized attempt to modify or disable the Endpoint Security Client.

Files Copied Alert Data

Lists accounts that have copied data to removable storage.

Incorrect Client Version Alert Data

Displays the history of the status of the ZENworks Security Client Update process.

Incorrect Client Policy Alert Data

Lists users who do not have the correct policy.

Override Attempts Alert Data

Lists instances where client self-defense mechanisms have been administratively overridden, granting privileged control over the Endpoint Security Client.

Integrity Failures Alert Data

Displays the history of success/failure client integrity checks.

Port Scan Alert Data

Lists the number of blocked packets on the number of different ports (a large number of ports may indicate a port scan occurred).

Uninstall Attempt Alert Data

Lists users who have attempted to uninstall the Endpoint Security Client.

Unsecure Access Point Alert Data

Lists unsecured access points detected by the Endpoint Security Client.

Unsecure Access Point Connection Alert Data

Lists unsecured access points connected to by the Endpoint Security Client.

5.5.4 Application Control Reports

Lists all unauthorized attempts by blocked applications to access the network or run when not permitted by the policy.

Click the plus sign next to *Alert Drill-Down Reports* to expand the list to display the following report:

- "Application Control Details" on page 56

Application Control Details

Lists the date, location, the action taken by the Endpoint Security Client, the application that attempted run, and the number of times this was attempted. Dates display in UTC.

Enter the date parameters, select the application names from the list, select the user accounts, and click *View* to run the report.

5.5.5 Endpoint Activity Reports

Endpoint Activity reports provide feedback for individual policy components and the effect they have on the operation of the endpoint.

Click the plus sign next to *Endpoint Activity* to expand the list to display the following reports:

- "Blocked Packets by IP Address" on page 56
- "Blocked Packets by User" on page 56
- "Network Usage Statistics by User" on page 57
- "Network Usage Statistics by Adapter Type" on page 57

Blocked Packets by IP Address

Lists blocked packets filtered by the destination IP address. Dates display in UTC.

Select the destination IP from the list and set the date parameters. The report displays the dates, locations, affected ports, and the name of the blocked packets.

Blocked Packets by User

Lists blocked packets filtered by users. Dates display in UTC. The data provided is essentially the same as *Blocked Packets by IP Address*, but arranged by user.

Network Usage Statistics by User

Lists packets sent, received, or blocked; and network errors, filtered by users. This report requires a range of dates to be entered. Dates display in UTC.

Network Usage Statistics by Adapter Type

Lists packets sent, received, or blocked; and network errors, filtered by adapter type. This report requires a range of dates to be entered and the Location. Dates display in UTC.

5.5.6 Encryption Solutions Reports

When endpoint encryption is activated, reports on the transference of files to and from the encrypted folders is monitored and recorded.

Click the plus sign next to *Encryption Solutions* to expand the list to display the following reports:

- "File Encryption Activity" on page 57
- "Encryption Exceptions" on page 57

File Encryption Activity

Lists files that have had encryption applied.

Encryption Exceptions

Lists errors from the encryption subsystem (for example, a protected file could not be decrypted because the user did not have the right keys).

5.5.7 Client Self Defense Reports

Client Self Defense reports provide feedback about users trying to prevent the Endpoint Security Client from doing its job.

Click the plus sign next to *Client Self Defense* to expand the list to display the following report:

- "Endpoint Security Client Hack Attempts" on page 57

Endpoint Security Client Hack Attempts

Lists instances where a user has made an unauthorized attempt to modify or disable the Endpoint Security Client. Dates display in UTC.

Specify the date parameters, then click *View* to run the report.

5.5.8 Integrity Enforcement Reports

Provides reporting for anti-virus/anti-spyware integrity results.

Click the plus sign next to *Integrity Enforcement* to expand the list to display the following reports:

- "Client Integrity History" on page 58

- "Unremediated Integrity Failures by Rule" on page 58
- "Unremediated Integrity Failures by User" on page 58

Client Integrity History

Lists the success and failure of client integrity checks. Dates display in UTC.

Select the date range for the report, integrity rule(s), and user name(s).

Unremediated Integrity Failures by Rule

Reports on integrity rules and tests that have failed and not yet been remediated.

Select the integrity rules, then click *View* to run the report.

Unremediated Integrity Failures by User

Reports on users that have failed integrity tests and not yet been remediated.

Select the user names, then click *View* to run the report.

5.5.9 Location Reports

Provides data for common location usage (which locations are most commonly used by users).

Click the plus sign next to *Location* to expand the list to display the following report:

- "Location Usage Data by Date and User" on page 58

Location Usage Data by Date and User

Displays information gathered from individual clients about what locations are used and when. Dates display in UTC. The locations displayed are the locations used by the user. Unused locations are not displayed. Select the date range to generate the report.

5.5.10 Outbound Content Compliance Reports

Provides information regarding the use of removable drives and identifies which files have been uploaded to such drives.

Click the plus sign next to *Outbound Content Compliance* to expand the list to display the following reports:

- "Removable Storage Activity by Account" on page 59
- "Removable Storage Activity by Device" on page 59
- "Copies from Removable Storage by Account" on page 59
- "Detected Removable Storage Devices" on page 59
- "Chart 7 Days of Removable Storage Activity by Account" on page 59

Removable Storage Activity by Account

Lists accounts that have copied data to removable storage. No parameters are required to generate this report.

Removable Storage Activity by Device

Shows removable storage devices to which files have been copied. Select the date range, user names, and locations to generate this report.

Copies from Removable Storage by Account

Shows accounts that have copied data from removable storage to fixed drives.

Detected Removable Storage Devices

Lists removable storage devices that have been detected on the endpoint. Select the date range, user names, and locations to generate this report.

Chart 7 Days of Removable Storage Activity by Account

Displays a chart listing accounts that have recently copied data to removable storage. Enter the date range to generate this report.

5.5.11 Administrative Overrides Reports

Reports instances where client self-defence mechanisms have been administratively overridden, granting privileged control over the Endpoint Security Client.

Click the plus sign next to *Administrative Overrides* to expand the list to display the following report:

- "Security Client Overrides" on page 59

Security Client Overrides

Displays successful override attempts by user and date. Dates display in UTC.

Select the user and date range, then click *View* to run the report.

5.5.12 Endpoint Updates Reports

Shows the status of the ZENworks Security Client Update process (see "ZSC Update" on page 94). Dates display in UTC.

Click the plus sign next to *Endpoint Updates* to expand the list to display the following reports:

- "Chart Percentage of ZSC Update Failures" on page 60
- "History of ZSC Update Status" on page 60
- "Chart Types of Failed ZSC Updates" on page 60

Chart Percentage of ZSC Update Failures

Lists the percentage of ZENworks Security Client Update that have failed (and not been remediated). No parameters are required to generate this report.

History of ZSC Update Status

Shows the history of the status of the ZENworks Security Client Update process. Select the date range and click *View* to run the report. The report displays the users that have checked in and received the update.

Chart Types of Failed ZSC Updates

Shows ZENworks Security Client Updates that have failed (and not been remediated). Select the date range and click *View* to run the report. The report displays the users that have checked in, but had a failed update installation.

5.5.13 USB Devices Reports

Shows security client USB device inventory that is listed by user or machine. This report shows whatever a user has plugged into a USB port and is recorded for either the user or the machine.

5.5.14 Wireless Enforcement Reports

Provides reports regarding Wi-Fi environments the endpoint is exposed to.

Click the plus sign next to *Wi-Fi Enforcement* to expand the list to display the following reports:

- "Wireless Connection Availability" on page 60
- "Wireless Connection Attempts" on page 60
- "Wireless Environment History" on page 60

Wireless Connection Availability

Displays the access points available for connection by policy and location. Includes the channel, SSID, MAC address, and whether or not the access point was encrypted.

Wireless Connection Attempts

Displays the access points connection attempts, by location and by ZENworks Endpoint Security Management account.

Wireless Environment History

Provides a survey of all detected access points, regardless of ownership. Includes the frequency, signal strength, and whether or not the access point was encrypted. Dates display in UTC. Select the desired locations and the date range to generate this report.

5.6 Generating Custom Reports

ZENworks Endpoint Security Management lets you create custom reports to better manage endpoint computers in your system.

The following sections contain more information:

- Section 5.6.1, "Software Requirements," on page 61
- Section 5.6.2, "Creating a ZENworks Endpoint Security Management Compliant Report," on page 61
- Section 5.6.3, "Available Reporting Information," on page 62
- Section 5.6.4, "Creating a Report," on page 65

5.6.1 Software Requirements

You can use ODBC-compliant reporting tools (for example, Crystal Reports*, Brio*, and Actuate*) to create custom reports not included in the Novell reports list. These reporting tools can view and query the reporting information from a common data warehouse, star format.

The reports included with ZENworks Endpoint Security Management were created using Crystal Reports for Visual Studio .NET (SP2). This version of Crystal Reports is bundled with Visual Studio .NET and is available as an optional component. To learn more, visit http://msdn.microsoft.com/vstudio/team/crystalreports/default.aspx (http://msdn.microsoft.com/vstudio/team/crystalreports/default.aspx).

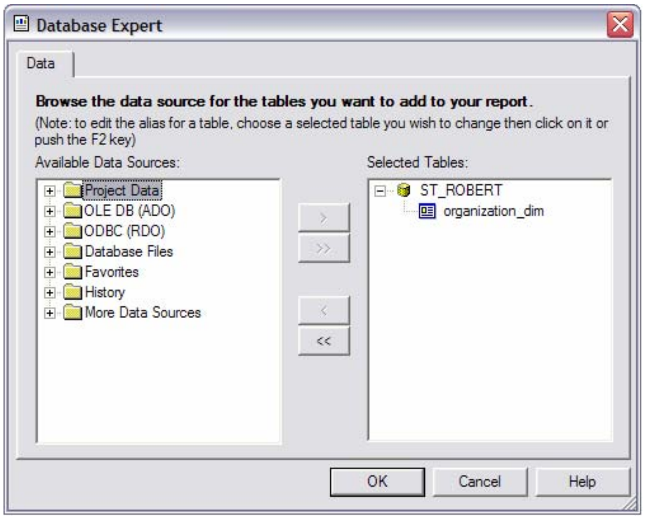
5.6.2 Creating a ZENworks Endpoint Security Management Compliant Report

Before you begin, please review the report creation process outlined at: http://msdn.microsoft.com/vstudio/team/crystalreports/gettingstarted/default.aspx (http://msdn.microsoft.com/vstudio/team/crystalreports/gettingstarted/default.aspx).

The first phase implementation of the ZENworks Endpoint Security Management reporting framework has the following requirements of every report to be integrated into the system:

- The report must be based on only one data source. That data source must be a single table or view residing within the source database.

Figure 5-13 *Browse the Reporting Data Source*

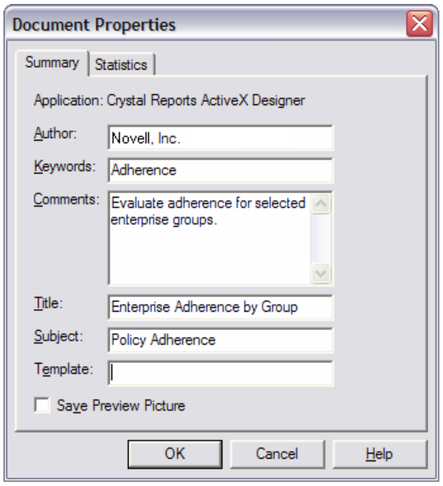


Browse the data source for the tables you want to add to your report.

(Note: to edit the alias for a table, choose a selected table you wish to change then click on it or push the F2 key)

- The report must have a title specified and saved with the report. The optional title, subject, author, and comments display if specified.

Figure 5-14 *Report Document Properties*



Application: Crystal Reports ActiveX Designer

Author: Novell, Inc.

Keywords: Adherence

Comments: Evaluate adherence for selected enterprise groups.

Title: Enterprise Adherence by Group

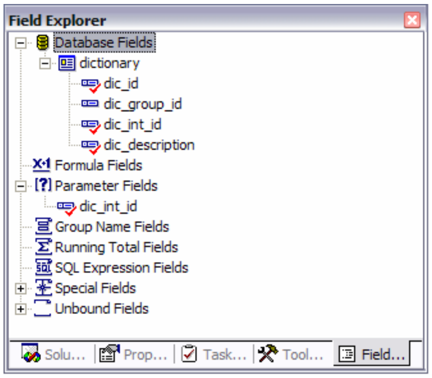
Subject: Policy Adherence

Template:

□ Save Preview Picture

- The report cannot contain any sub-reports.
- Filtering parameters must be named the same as the target columns within the database fields of the table or view.

Figure 5-15 *Available Database Fields*



- Database Fields
  - dictionary
    - dic_id
    - dic_group_id
    - dic_int_id
    - dic_description
- Formula Fields
- Parameter Fields
  - dic_int_id
- Group Name Fields
- Running Total Fields
- SQL Expression Fields
- Special Fields
- Unbound Fields

5.6.3 Available Reporting Information

The ZENworks Endpoint Security Management reporting database is designed to closely model the star schema format. The star schema is a single "fact" table containing a compound primary key, with one segment for each dimension and additional columns of additive, numeric facts.

The Reporting Service includes the following two dimension tables:

ORGANIZATION_DIM: The organization table, defining the instances of users, groups, organizational units, containers, and services in a hierarchal relationship. Each row represents one of these units.

UNIT_MEMBER_DIM: Association of organization units to other organization units. For example, although a user can be stored within a specific container within Active Directory, the user might also be a member of an organization unit or security groups. Each row represents a relationship of organization units.

The data source must be defined to the reporting tool, typically for most third-party applications the following steps are necessary:

1. Define an OLEDB ADO connection to the server hosting the Management Service.
2. Select the Microsoft OLE DB Provider for SQL Server.
3. Enter the Management Service server as the server.
4. Enter the SQL account name and password.
5. Enter the Reporting Service database name (default name is STRSDB) as the database.

The following views are available for report generation:

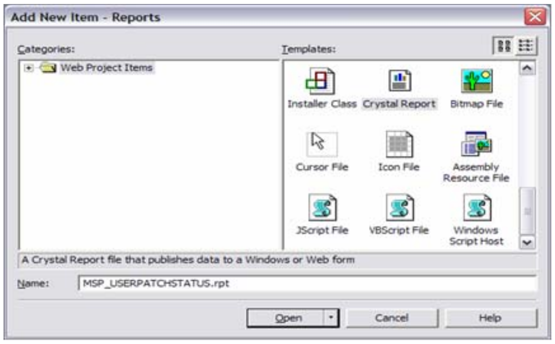
- **EVENT_ACCESSPOINT_FACT_VW:** This view describes the access points observed by user, day, policy, location, and access point instance.
- **EVENT_BLOCKEDPACKETS_FACT_VW:** This view describes the summarized instances of port activity that was blocked due to policy configuration by the endpoint. The information included is logged user, day, policy, location, and source/destination IP/port.
- **EVENT_CLIENTACTIVITY_FACT_VW:** This view describes the summarized instances of port activity at the endpoint. The information included is logged user, day, policy, location and device.
- **EVENT_CLIENTAPPLICATIONS_FACT_VW:** This view describes the summarized instances of application use (duration) by user, day, policy, location and application.
- **EVENT_CLIENTDEFENSE_HACK_FACT_VW:** This view describes the instances of hack attempts against the endpoint client. Active users, applications, and services are included within the report. The data is grouped by user, day, policy, location, and attack result.
- **EVENT_CLIENTDEFENSE_OVERRIDES_FACT_VW:** This view describes the instances of policy override and the affected devices. The data is grouped by user, day, policy, location, and override type.
- **EVENT_CLIENTDEFENSE_UNINSTALL_FACT_VW:** This view describes the instances of attempts to remove the endpoint client. The data is grouped by user, day, policy, location, and attack result.
- **EVENT_CLIENTDEVICE_FACT_VW:** This view describes the types of devices in use by an endpoint. The data is grouped by user, day, policy, location, and device type.
- **EVENT_CLIENTENVIRONMENTS_FACT_VW:** This view describes the custom (stamped) network environments used for location detection. The data is grouped by user, day, policy, location, device type, and environment data.
- **EVENT_CLIENTINTEGRITY_FACT_VW:** This view describes the results of integrity rules applied at the endpoint. The data is grouped by user, day, policy, location, and rule.
- **EVENT_CLIENTLOCATION_FACT_VW:** This view describes the time at location as well as adapter (configuration and type) used at the location. The data is grouped by user, day, policy, and location.
- **EVENT_CLIENTRULE_FACT_VW:** This view describes the generic reporting mechanism for integrity and scripting rules. The data is grouped by user, day, policy, location, and rule.
- **EVENT_COMPONENTACTION_FACT_VW:** This view describes the Management Console activity performed on specific components. For example, you could see when the policy update interval was changed for a specific location in a policy. The data is grouped by user, day, policy, and component and defines the new and old value.
- **EVENT_MANGERIO_FACT_VW:** This view describes when a component has been created or edited. The data is grouped by user, day, component, and action.
- **EVENT_ORGANIZATIONACTION_FACT_VW:** This view describes the user activity as it relates to ZENworks Endpoint Security Management integration with an Enterprise information repository. All user management activities are reflected within this table.

- **EVENT_POLICYCOMPONENT_FACT_VW:** This view describes the interaction of components and policies. For example, when a location is added to a policy, an audit row reflects that change. The data is grouped by user, day, policy, component, and action.
- **EVENT_PUBLISHACTION_FACT_VW:** This view describes the policy and component assignment to an organization.
- **EVENT_SERVERACTION_FACT_VW:** This view describes the user activity with the Distribution Service (Check In, for example).
- **EVENT_USERACTION_FACT_VW:** This view describes the user policy activity with the Distribution Service (Policy, Key, EFS Key, Schema downloads).

5.6.4 Creating a Report

The following steps describe the creation of a simple report. The following example uses the Visual Studio.NET 2003 Enterprise Architect IDE.

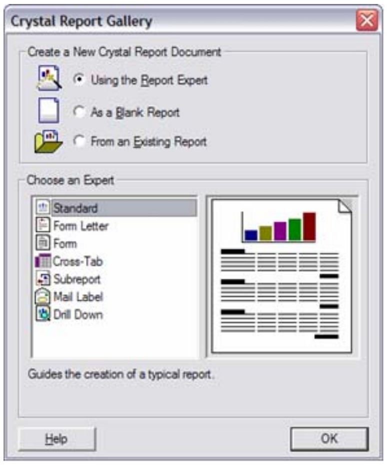
1 From the IDE, select *Add New Item* and add a new Crystal Report.



A Crystal Report file that publishes data to a Windows or Web form

Name: MSP_USERPATCHSTATUS.rpt

2 Create a report using the wizard.

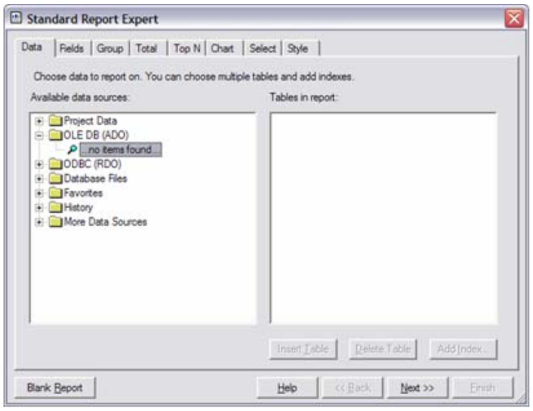


Create a New Crystal Report Document: ● Using the Report Expert

Choose an Expert: Standard

Guides the creation of a typical report.

3 Define the data source. Access the Management Service reporting service database within data.



Standard Report Expert

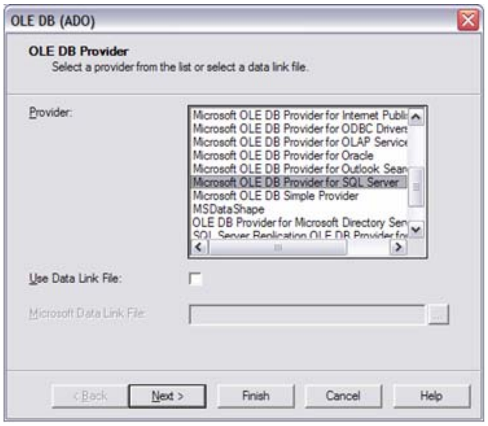
Choose data to report on. You can choose multiple tables and add indexes.

Available data sources:

- Project Data
- OLE DB (ADO)
  - ...no items found...
- ODBC (RDO)
- Database Files
- Favorites
- History
- More Data Sources

Tables in report:

4 Using the connection definition wizard, define an OLEDB ADO connection to the Reporting Service database. Select *Microsoft OLE DB Provider for SQL Server*, then click *Next*.



OLE DB (ADO)

OLE DB Provider

Select a provider from the list or select a data link file.

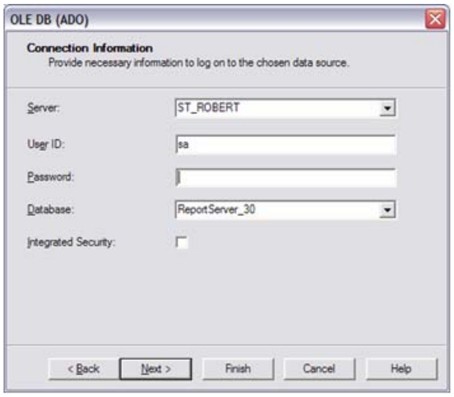
Provider:

- Microsoft OLE DB Provider for Internet Publi
- Microsoft OLE DB Provider for ODBC Drivers
- Microsoft OLE DB Provider for OLAP Service
- Microsoft OLE DB Provider for Oracle
- Microsoft OLE DB Provider for Outlook Searc
- Microsoft OLE DB Provider for SQL Server
- Microsoft OLE DB Simple Provider
- MSDataShape
- OLE DB Provider for Microsoft Directory Ser
- SQL Server Replication OLE DB Provider for

Use Data Link File: □

Microsoft Data Link File:

5 Select the Reporting server. Enter the User ID, password, and database name for the Reporting Service (see the *ZENworks Endpoint Security Management Installation Guide* for more information). Click *Next,* then click *Finish*.



OLE DB (ADO)

Connection Information

Provide necessary information to log on to the chosen data source.

Server: ST_ROBERT

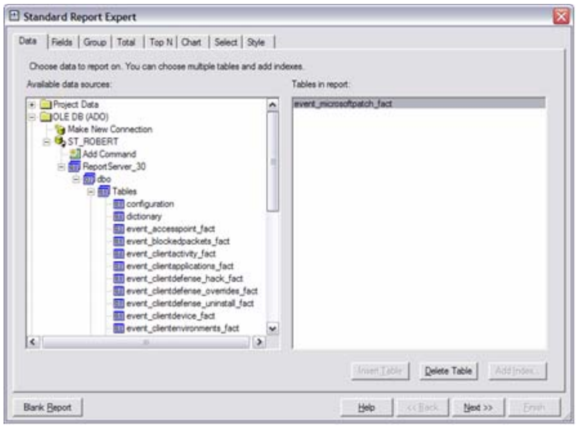
User ID: sa

Password:

Database: ReportServer_30

Integrated Security: □

6 Select the desired source table or view for your report by expanding the tree nodes as shown below.



Choose data to report on. You can choose multiple tables and add indexes.

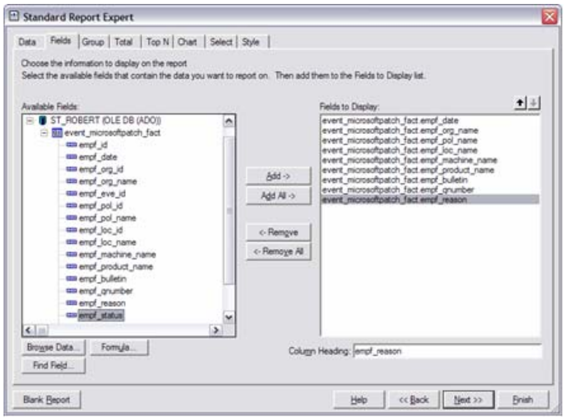
Available data sources:

- Project Data
- OLE DB (ADO)
  - Make New Connection
  - ST_ROBERT
    - Add Command
    - ReportServer_30
      - dbo
        - Tables
          - configuration
          - dictionary
          - event_accesspoint_fact
          - event_blockedpackets_fact
          - event_clientactivity_fact
          - event_clientapplications_fact
          - event_clientdefense_hack_fact
          - event_clientdefense_overrides_fact
          - event_clientdefense_uninstall_fact
          - event_clientdevice_fact
          - event_clientenvironments_fact

Tables in report:

event_microsoftpatch_fact

7 Under the *Fields* tab, select the table or view columns that you want to include within your report. Click *Next* to continue.



Choose the information to display on the report

Select the available fields that contain the data you want to report on. Then add them to the Fields to Display list.

Available Fields:

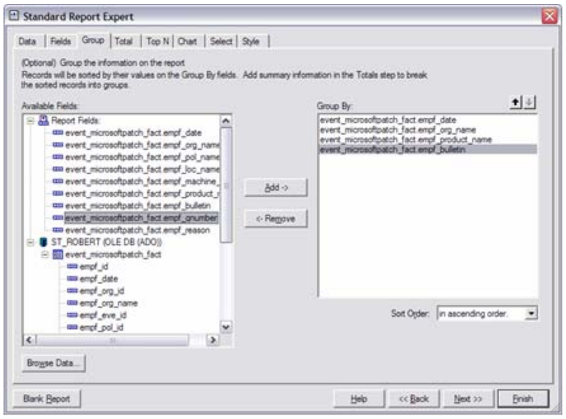
- ST_ROBERT (OLE DB (ADO))
  - event_microsoftpatch_fact
    - empf_id
    - empf_date
    - empf_org_id
    - empf_org_name
    - empf_eve_id
    - empf_pol_id
    - empf_pol_name
    - empf_loc_id
    - empf_loc_name
    - empf_machine_name
    - empf_product_name
    - empf_bulletin
    - empf_qnumber
    - empf_reason
    - empf_status

Fields to Display:

event_microsoftpatch_fact.empf_date
event_microsoftpatch_fact.empf_org_name
event_microsoftpatch_fact.empf_pol_name
event_microsoftpatch_fact.empf_loc_name
event_microsoftpatch_fact.empf_machine_name
event_microsoftpatch_fact.empf_product_name
event_microsoftpatch_fact.empf_bulletin
event_microsoftpatch_fact.empf_qnumber
event_microsoftpatch_fact.empf_reason

Column Heading: empf_reason

8 If you are planning to group or summarize your data, click the *Group* tab and select the columns you want to group. Click *Next* or select the *Style* tab.



(Optional) Group the information on the report

Records will be sorted by their values on the Group By fields. Add summary information in the Totals step to break the sorted records into groups.

Available Fields:

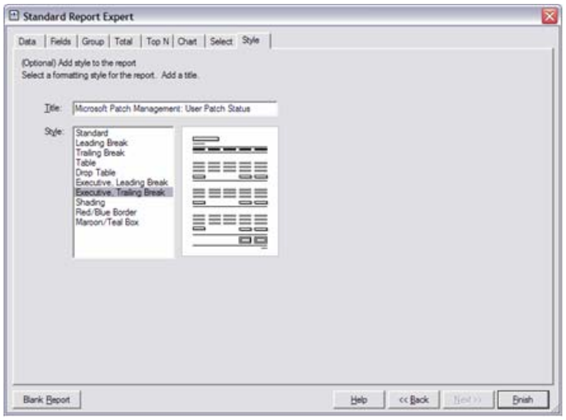
- Report Fields:
  - event_microsoftpatch_fact.empf_date
  - event_microsoftpatch_fact.empf_org_name
  - event_microsoftpatch_fact.empf_pol_name
  - event_microsoftpatch_fact.empf_loc_name
  - event_microsoftpatch_fact.empf_machine_
  - event_microsoftpatch_fact.empf_product_
  - event_microsoftpatch_fact.empf_bulletin
  - event_microsoftpatch_fact.empf_qnumber
  - event_microsoftpatch_fact.empf_reason
- ST_ROBERT (OLE DB (ADO))
  - event_microsoftpatch_fact
    - empf_id
    - empf_date
    - empf_org_id
    - empf_org_name
    - empf_eve_id
    - empf_pol_id

Group By:

event_microsoftpatch_fact.empf_date
event_microsoftpatch_fact.empf_org_name
event_microsoftpatch_fact.empf_product_name
event_microsoftpatch_fact.empf_bulletin

Sort Order: in ascending order.

9 Title the report and select the style.

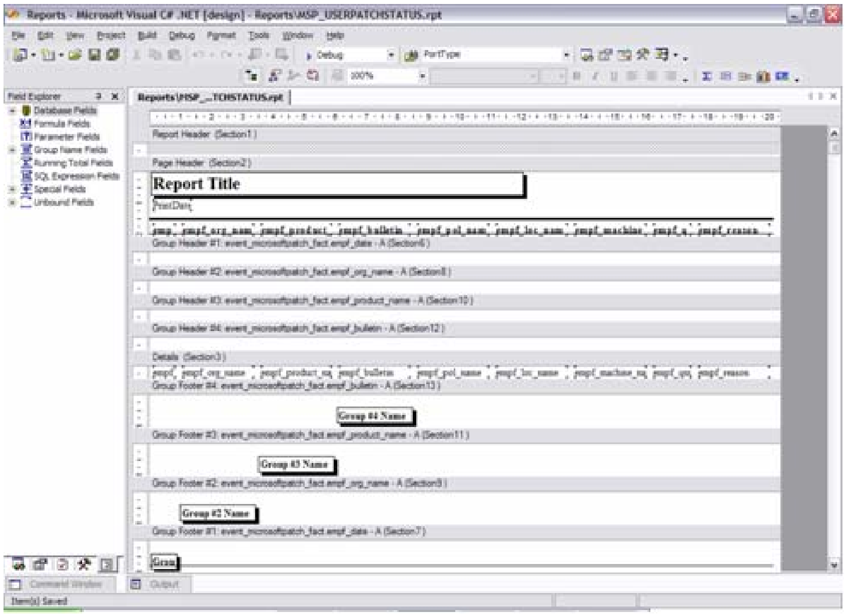


(Optional) Add style to the report
Select a formatting style for the report. Add a title.

Title: Microsoft Patch Management: User Patch Status

Style:
- Standard
- Leading Break
- Trailing Break
- Table
- Drop Table
- Executive, Leading Break
- Executive, Trailing Break
- Shading
- Red/Blue Border
- Maroon/Teal Box

The Report Builder displays.



Report Header (Section1)

Page Header (Section2)

Report Title

PrintDate

Group Header #1: event_microsoftpatch_fact.empf_date - A (Section6)

Group Header #2: event_microsoftpatch_fact.empf_org_name - A (Section8)

Group Header #3: event_microsoftpatch_fact.empf_product_name - A (Section10)

Group Header #4: event_microsoftpatch_fact.empf_bulletin - A (Section12)

Details (Section3)

Group Footer #4: event_microsoftpatch_fact.empf_bulletin - A (Section13)

Group #4 Name

Group Footer #3: event_microsoftpatch_fact.empf_product_name - A (Section11)

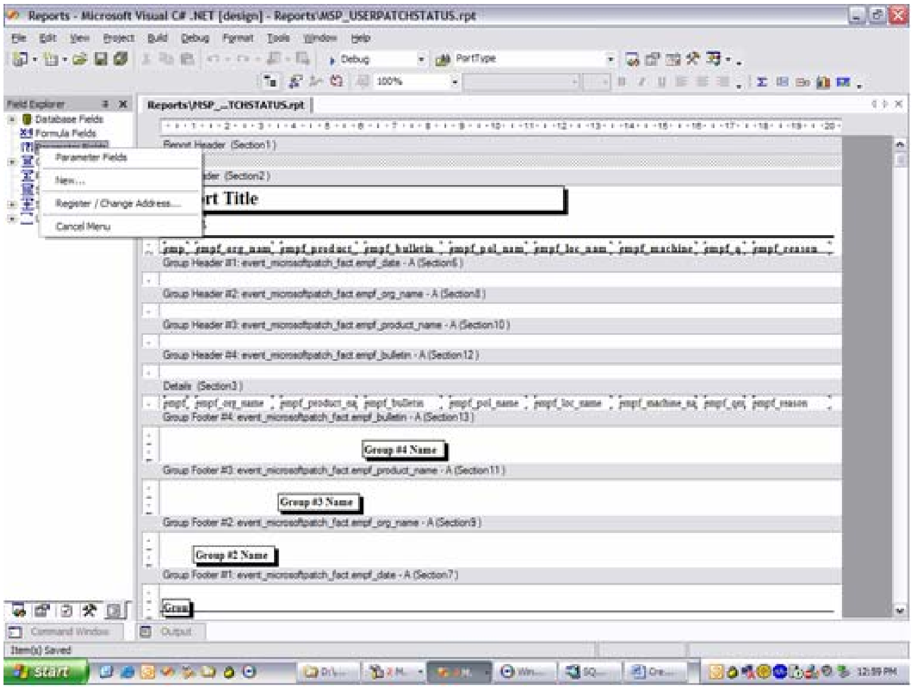
Group #3 Name

Group Footer #2: event_microsoftpatch_fact.empf_org_name - A (Section9)

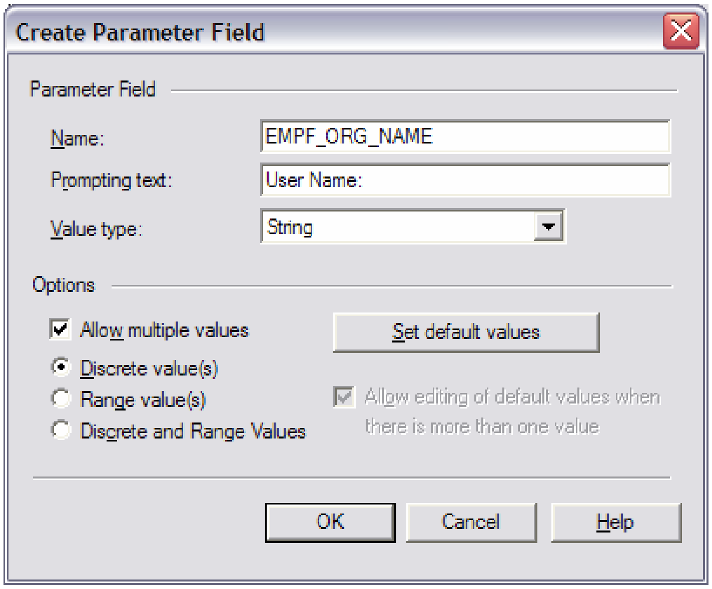
Group #2 Name

Group Footer #1: event_microsoftpatch_fact.empf_date - A (Section7)

10 To set up a filter, right-click *Parameter Fields* in the field explorer, then click *New*.


Reports - Microsoft Visual C# .NET [design] - Reports\MSP_USERPATCHSTATUS.rpt
Field Explorer
Database Fields
Formula Fields
Parameter Fields
New...
Register / Change Address...
Cancel Menu
Reports\MSP_...TCHSTATUS.rpt
Report Header (Section1)
Report Title
Group Header #1: event_microsoftpatch_fact.empf_date - A (Section6)
Group Header #2: event_microsoftpatch_fact.empf_org_name - A (Section8)
Group Header #3: event_microsoftpatch_fact.empf_product_name - A (Section10)
Group Header #4: event_microsoftpatch_fact.empf_bulletin - A (Section12)
Details (Section3)
Group Footer #4: event_microsoftpatch_fact.empf_bulletin - A (Section13)
Group #4 Name
Group Footer #3: event_microsoftpatch_fact.empf_product_name - A (Section11)
Group #3 Name
Group Footer #2: event_microsoftpatch_fact.empf_org_name - A (Section9)
Group #2 Name
Group Footer #1: event_microsoftpatch_fact.empf_date - A (Section7)
Item(s) Saved
start
12:59 PM

11 The following filter allows you to select multiple users to filter by with the prompting text of "User Name:" displayed within the UI. The parameter is named the same as the column.



Create Parameter Field

Parameter Field

Name: EMPF_ORG_NAME

Prompting text: User Name:

Value type: String

Options

☑ Allow multiple values

● Discrete value(s)

○ Range value(s)

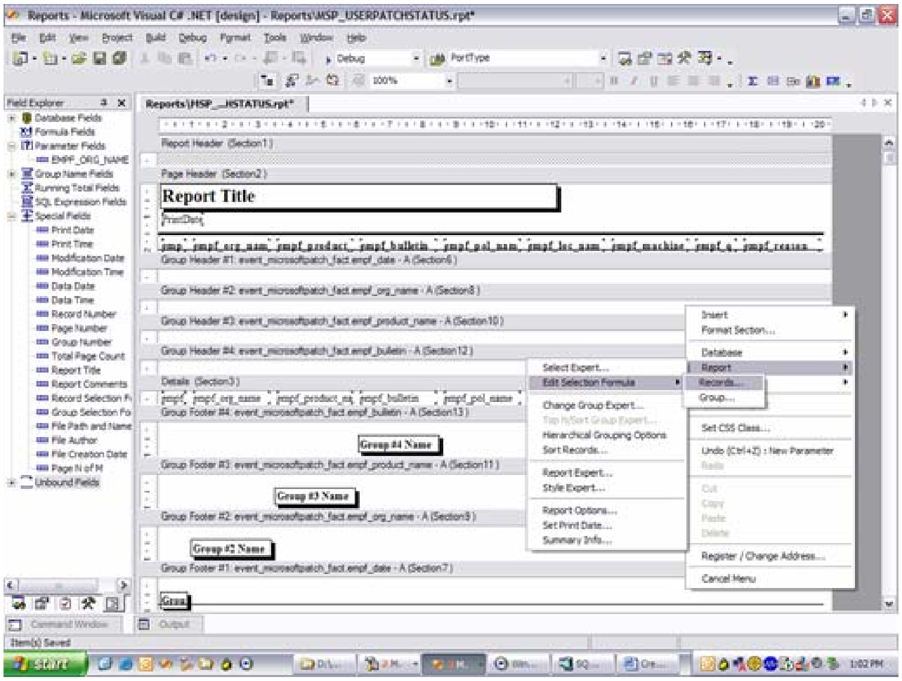
○ Discrete and Range Values

Set default values

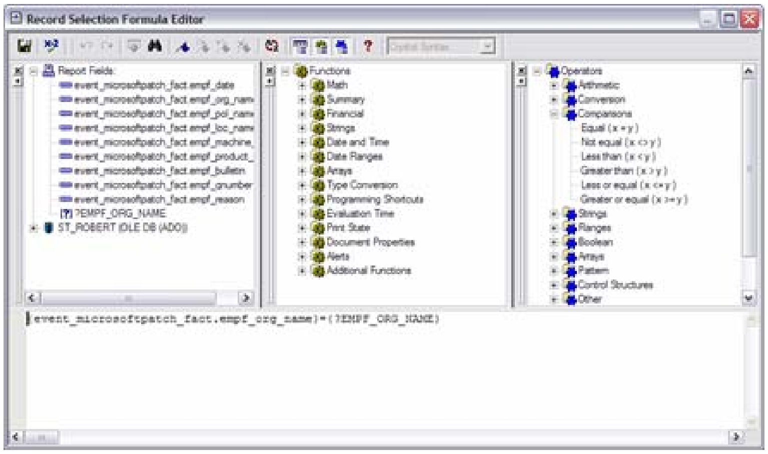
☑ Allow editing of default values when there is more than one value

OK | Cancel | Help

12 Right-click the report, then click *Report* > *Edit Selection Formula* > *Records*.


Reports - Microsoft Visual C# .NET [design] - Reports\MSP_USERPATCHSTATUS.rpt*
Field Explorer
Database Fields
Formula Fields
Parameter Fields
EMPF_ORG_NAME
Group Name Fields
Running Total Fields
SQL Expression Fields
Special Fields
Report Header (Section1)
Page Header (Section2)
Report Title
Group Header #1: event_microsoftpatch_fact.empf_date - A (Section6)
Group Header #2: event_microsoftpatch_fact.empf_org_name - A (Section8)
Group Header #3: event_microsoftpatch_fact.empf_product_name - A (Section10)
Group Header #4: event_microsoftpatch_fact.empf_bulletin - A (Section12)
Details (Section3)
Group Footer #4: event_microsoftpatch_fact.empf_bulletin - A (Section13)
Group #4 Name
Group Footer #3: event_microsoftpatch_fact.empf_product_name - A (Section11)
Group #3 Name
Group Footer #2: event_microsoftpatch_fact.empf_org_name - A (Section9)
Group #2 Name
Group Footer #1: event_microsoftpatch_fact.empf_date - A (Section7)
Select Expert...
Edit Selection Formula
Change Group Expert...
Hierarchical Grouping Options
Sort Records...
Report Expert...
Style Expert...
Report Options...
Set Print Date...
Summary Info...
Insert
Format Section...
Database
Report
Records...
Group...
Set CSS Class...
Undo (Ctrl+Z) : New Parameter
Redo
Cut
Copy
Paste
Delete
Register / Change Address...
Cancel Menu
Start

13 Using the new parameter, specify only the records where the field equals the values selected in the parameter. Select the column and then a comparison (=) and then the parameter. Press CTRL-S to save the filter



```
event_microsoftpatch_fact.empf_org_name)=(?EMPF_ORG_NAME)
```

14 Repeat Step 10 to Step 13 for each filter. Edit the design of the report and the save the report.

15 After a custom report is generated, the report can be dropped into the `\Program Files\Novell\Management Service\Reports\Reports\` directory on the Management Service Server. Once there, the new report displays in the reports list in the Reporting Service web interface (click *Refresh List* to display the new reports).

5.7 Using the ZENworks Storage Encryption Solution

The ZENworks Storage Encryption Solution provides complete, centralized security management of all mobile data by actively enforcing a corporate encryption policy on the endpoint itself.

The ZENworks Storage Encryption Solution lets you do the following:

- Centrally create, distribute, enforce, and audit encryption policies on all endpoints and removable storage devices.
- Encrypt all files saved to, or copied to, a specific directory on all fixed disc partitions on the hard drive.
- Encrypt all files copied to removable storage devices.
- Share files freely within an organization, while blocking unauthorized access to files.
- Share password-protected, encrypted files with people outside the organization through an available decryption utility.
- Easily update, back up, and recover keys via policy without losing data.

The following sections contain additional information:

- Section 5.7.1, "Understanding the ZENworks Storage Encryption Solution," on page 71
- Section 5.7.2, "Sharing Encrypted Files," on page 71

5.7.1 Understanding the ZENworks Storage Encryption Solution

Data encryption is enforced on fixed disk volumes and removable storage devices through the creation and distribution of data encryption security policies.

When a data encryption policy is activated on an endpoint device, an encrypted Safe Harbor folder is added to the root directory of any fixed disk volumes on the endpoint. Any data stored in a Safe Harbor folder is encrypted. Attempts to read the data by anyone who is not an authorized user for that endpoint device are unsuccessful.

Any removable storage device connected to the device is encrypted. Data placed on the removable storage device is immediately encrypted and can only be read on endpoint devices in the same policy group. If desired, you can configure the policy to provide a sharing folder (the default name is Password Encrypted Files) on the removable storage devices. This folder enables users to share the folder's files with persons outside their policy group via a password (see "Data Encryption" on page 91).

5.7.2 Sharing Encrypted Files

Each Management Console contains its own encryption key. Users assigned policies created by the same Management Console can access encrypted files created by each other. For example, if User A and User B are assigned data encryption policies created with the same Management Console, User A can log in to User B's machine (as User A) and access User B's encrypted files. User A can also read any files on an encrypted removable storage device supplied by User B.

Users assigned policies created by different Management Consoles cannot access each other's fixed disk encrypted files unless you share (export and import) encryption keys between consoles. The same is true of files on an encrypted removable storage device, with the exception of files located in the Password Encrypted Files (shared) folder. For files located in the shared folder, the user must provide the access password.

If an endpoint device does not have the Security client installed, users of the device can access shared folder files from an encrypted removable device if 1) they have the ZENworks File Decryption Utility and 2) they know the file access password. For information about the File Decryption Utility, see Section 9.1, "Using the ZENworks File Decryption Utility," on page 203.

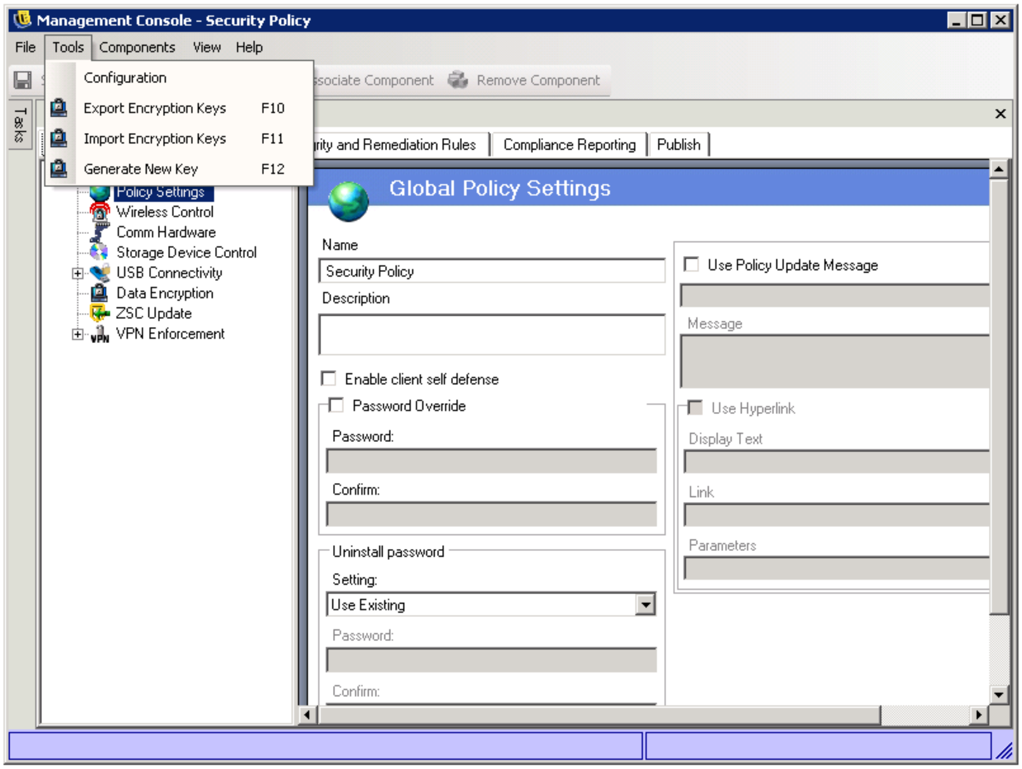
5.8 Managing Keys

Key management permits you to back up, import, and update an encryption key. We recommend the following key management practices:

- Export and save your encryption keys. This ensures that, in the case of a systems failure or an inadvertent policy change, data can be decrypted. Each Management Console has its own encryption key. If you have multiple Management Consoles, you need to export the encryption key from each console.
- If you believe that an encryption key is compromised, update to a new key. Generating a new key results in a temporary performance decrease on endpoint devices while the Security client reencrypts data.
- If you have used multiple Management Consoles to create Data Encryption policies, you should export the key from each Management Console and import it into the other consoles so that all Management Consoles have all keys. This allows the Management Console to include all keys in each Data Encryption policy. The result is that all Security client users, regardless of their Data Encryption policy, can access encrypted policies created by other Security client users in your environment.

Encryption Key controls are accessed through the *Tools* menu of the ZENworks Endpoint Security Management Console.

Figure 5-16 *Access Encryption Keys through the tools menu*



Name: Security Policy

Description:

□ Enable client self defense

□ Password Override

Password:

Confirm:

Uninstall password

Setting: Use Existing

Password:

Confirm:

□ Use Policy Update Message

Message

□ Use Hyperlink

Display Text

Link

Parameters

The following sections contain additional information:

- Section 5.8.1, “Exporting Encryption Keys,” on page 73
- Section 5.8.2, “Importing Encryption Keys,” on page 74
- Section 5.8.3, “Generating a New Key,” on page 74

5.8.1 Exporting Encryption Keys

For back up purposes, and to send the key to another Management Console, the current encryption key set can be exported to a designated file location.

1. In the Management Console, click *Tools*, then click *Export Encryption Keys*.
2. Specify the path and filename for the exported file.
3. Specify a password in the provided field. The key cannot be imported without this password.
4. Click *OK*.

All key files in the database are included in the exported file.

5.8.2 Importing Encryption Keys

You can import keys from a backup or another Management Console. Importing keys from another Management Console allows endpoints managed by this console to read files protected by Data Encryption policies created in the other Management Console. When importing keys, duplicates are ignored. Imported keys become part of your “key set” and do not replace the current common key. All keys are passed down when a new policy is published.

1. In the Management Console, click *Tools*, then click *Import Encryption Keys*.
2. Browse to or specify the file to be imported.
3. Specify the password for the encryption key.
4. Click *OK*.

5.8.3 Generating a New Key

1. In the Management Console, click *Tools*, then click *Generate New Key*.

All previous keys are stored in the policy.

Creating and Distributing Security Policies

6

The ZENworks® Endpoint Security Client uses security policies to apply location security to mobile users. Decisions on networking port availability, network application availability, file storage device access, and wired or Wi-Fi connectivity are determined by the administrator for each location.

Security policies can be custom-created for the enterprise, individual user groups, or individual users/machines. Security policies can allow full employee productivity while securing the endpoint, or can restrict the employee to only running certain applications and having only authorized hardware available to them.

IMPORTANT: Information in this section that pertains to the Endpoint Security Client has been written for the Endpoint Security Client 3.5. For the features that are supported in Endpoint Security Client 4.0, see the "Novell ZENworks Endpoint Security Client 4.0" Readme.

The following sections contain more information:

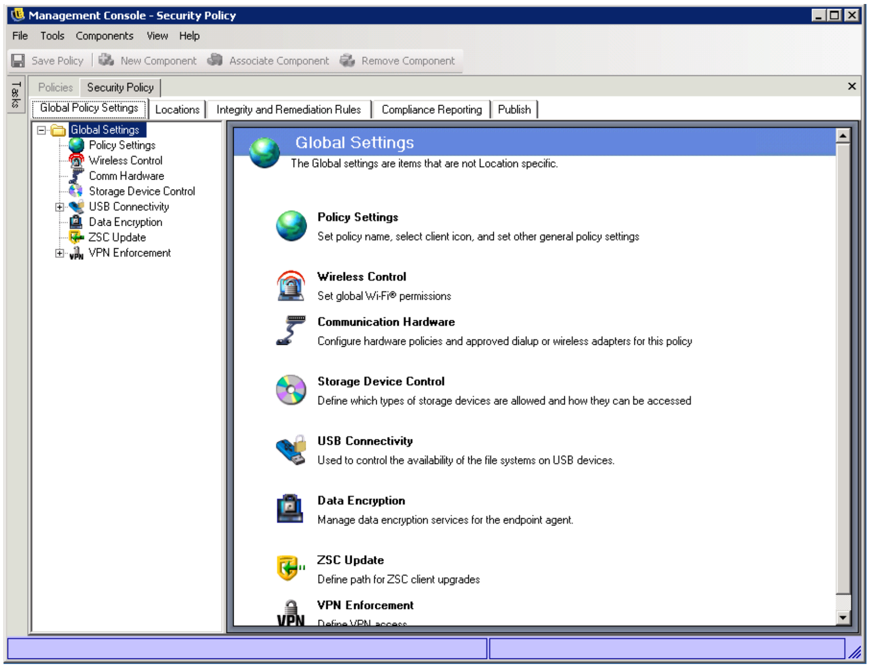
- Section 6.1, "Navigating the Management Console UI," on page 75
- Section 6.2, "Creating Security Policies," on page 79
- Section 6.3, "Managing Policies," on page 122
- Section 6.4, "Importing and Exporting Policies," on page 169
- Section 6.5, "Sample Scripts," on page 170

6.1 Navigating the Management Console UI

To begin a security policy:

1 In the Management Console, click *File* > *Create New Policy*.

2 Specify the name for the new policy, then click *Create* to display the Management Console with the Policy toolbar and the *Policy* tab displayed.



Global Settings
The Global settings are items that are not Location specific.

Policy Settings
Set policy name, select client icon, and set other general policy settings

Wireless Control
Set global Wi-Fi® permissions

Communication Hardware
Configure hardware policies and approved dialup or wireless adapters for this policy

Storage Device Control
Define which types of storage devices are allowed and how they can be accessed

USB Connectivity
Used to control the availability of the file systems on USB devices.

Data Encryption
Manage data encryption services for the endpoint agent.

ZSC Update
Define path for ZSC client upgrades

VPN Enforcement
Define VPN access

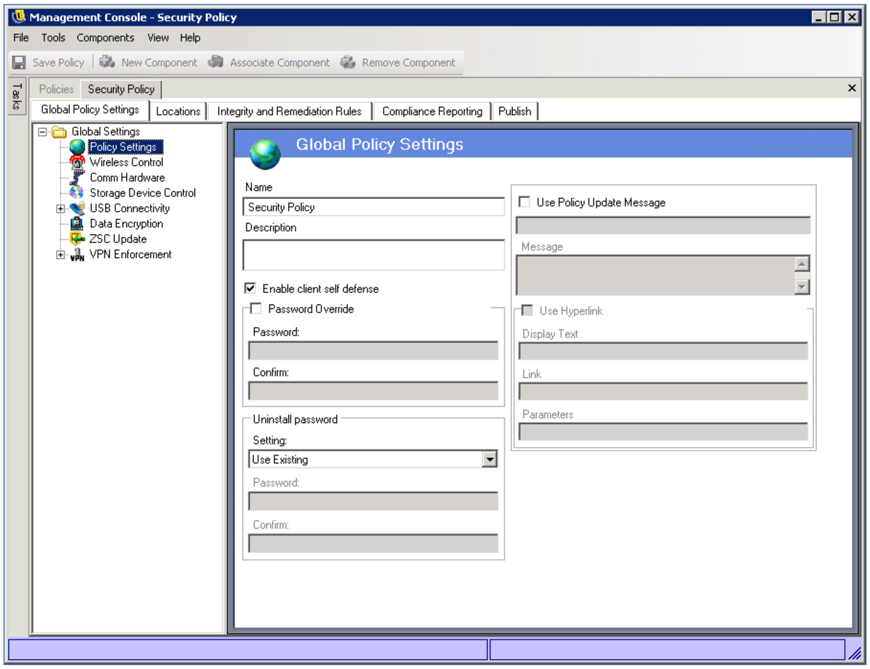
The following sections describe the Management Console's user interface as it relates to creating and distributing security policies using ZENworks Endpoint Security Management:

- Section 6.1.1, "Using the Policy Tabs and Tree," on page 76
- Section 6.1.2, "Using the Policy Toolbar," on page 78

6.1.1 Using the Policy Tabs and Tree

A security policy is configured by navigating through the available tabs at the top of the Management Console and by using the options in the *Global Settings* tree in the left pane.

Figure 6-1 Management Console



Name: Security Policy

Description:

☑ Enable client self defense

□ Password Override

Password:

Confirm:

Uninstall password

Setting: Use Existing

Password:

Confirm:

□ Use Policy Update Message

Message

□ Use Hyperlink

Display Text

Link

Parameters

The available tabs include the following:

- **Global Policy Settings:** The Global Policy Settings are applied as defaults throughout the policy and are not location specific.

  The Global Policy Settings let you configure the following settings:

  - Policy Settings
  - Wireless Control
  - Communication Hardware
  - Storage Device Control
  - USB Connectivity
  - Data Encryption
  - Endpoint Security Client
  - VPN Enforcement

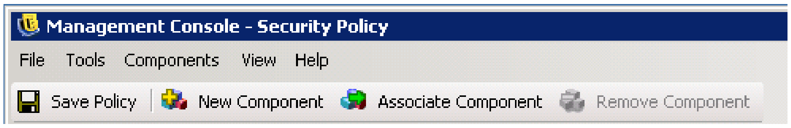
- **Locations:** These policy rules are applied within a specific location type, whether specified as a single network or a type of network, such as a coffee shop or airport.
- **Integrity and Remediation Rules:** These rules ensure that essential software (such as antivirus and spyware) is running and up-to-date on the device.
- **Compliance Reporting:** Instructs the policy whether reporting data (including the type of data) is gathered for this particular policy.
- **Publish:** Publishes the completed policy to individual users, directory service user groups, and individual machines.

The Policy Tree displays the available subset components for the tabbed categories. For example, *Global Policy Settings* include subsets of *Wireless Control*, *ZENworks Security Client Update*, and *VPN Enforcement*. Only the items contained on the primary subset page are required to define a category, the remaining subsets are optional components.

6.1.2 Using the Policy Toolbar

The policy toolbar provides four controls. The *Save* control is available throughout policy creation; the component controls are only available under the *Locations* and *Integrity and Remediation* tabs.

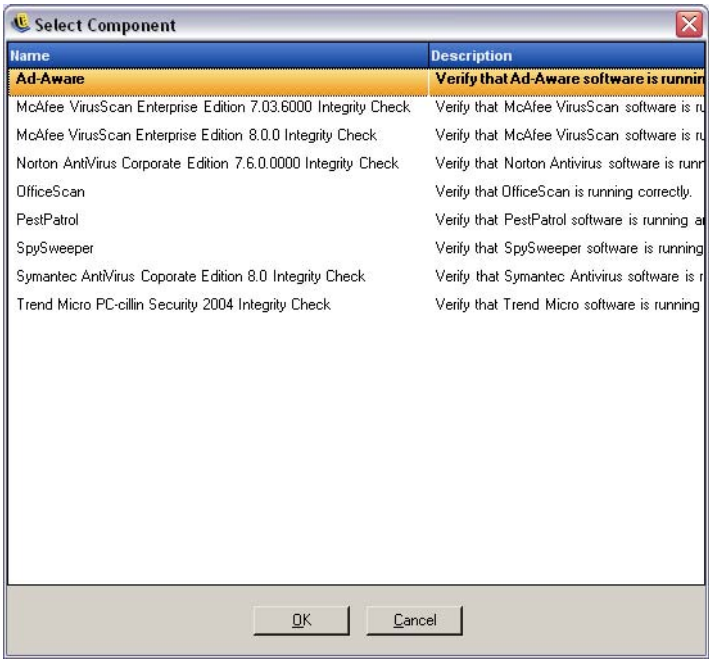
Figure 6-2 *Policy Toolbar*



Explanations of the tools are provided below:

- **Save Polic:** Saves the policy in its current state. As you complete each component subset, it is highly recommended that you click the *Save* icon on the *Policy* toolbar. If incomplete or incorrect data is entered into a component, the error notification screen displays (see Section 6.3.2, “Error Notification,” on page 122 for more details).
- **New Component:** Creates a new component in a Location or Integrity subset. After the policy is saved, a new component is available to associate in other policies.
- **Associate Component:** Opens the Select Component screen for the current subset. The available components include any pre-defined components included at installation and all components created in other policies.

Figure 6-3 *Select Component Window*



Name	Description
Ad-Aware	Verify that Ad-Aware software is runnir
McAfee VirusScan Enterprise Edition 7.03.6000 Integrity Check	Verify that McAfee VirusScan software is ru
McAfee VirusScan Enterprise Edition 8.0.0 Integrity Check	Verify that McAfee VirusScan software is ru
Norton AntiVirus Corporate Edition 7.6.0.0000 Integrity Check	Verify that Norton Antivirus software is runr
OfficeScan	Verify that OfficeScan is running correctly.
PestPatrol	Verify that PestPatrol software is running a
SpySweeper	Verify that SpySweeper software is running
Symantec AntiVirus Coporate Edition 8.0 Integrity Check	Verify that Symantec Antivirus software is r
Trend Micro PC-cillin Security 2004 Integrity Check	Verify that Trend Micro software is running

Changes made to associated components affect all other instances of that component. For example, you can create a single Location component named Work that defines the corporate network environment and security settings to be applied whenever an endpoint enters that environment. This component can now be applied to all security policies. Updates to the environment or security settings can be changed in the component in one policy and will update the same component in all other policies that its associated to.

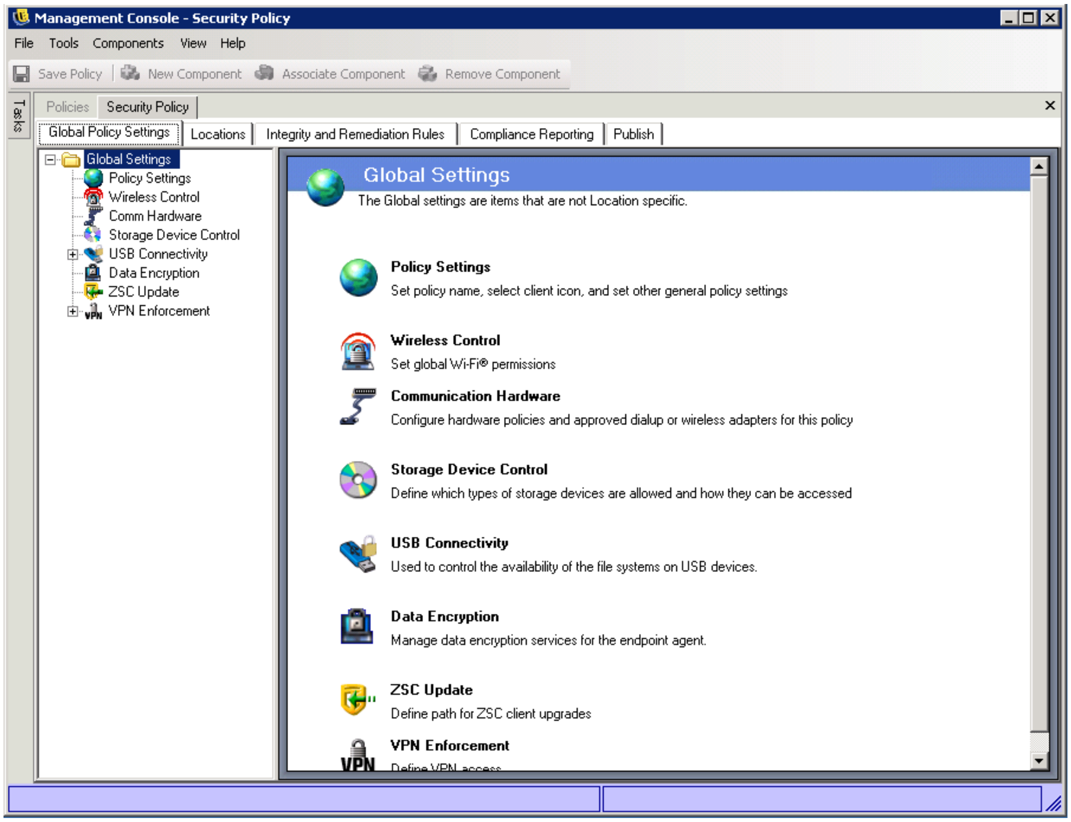
Use the *Show Usage* command to view all other policies associated with this component.

- **Remove Component:** Removes a component from the policy. The component is still available for association in this and other policies.

6.2 Creating Security Policies

To begin a security policy:

1. In the Management Console, click *File* > *Create New Policy*.
2. Specify the name for the new policy, then click *Create* to display the Management Console with the Policy toolbar and the Policy tabs displayed.



Global Settings

The Global settings are items that are not Location specific.

Policy Settings
Set policy name, select client icon, and set other general policy settings

Wireless Control
Set global Wi-Fi® permissions

Communication Hardware
Configure hardware policies and approved dialup or wireless adapters for this policy

Storage Device Control
Define which types of storage devices are allowed and how they can be accessed

USB Connectivity
Used to control the availability of the file systems on USB devices.

Data Encryption
Manage data encryption services for the endpoint agent.

ZSC Update
Define path for ZSC client upgrades

VPN Enforcement
Define VPN access

3. Configure the policy settings using the following tabs (click each link for detailed information about each tab and its options):

- Section 6.2.1, “Global Policy Settings,” on page 80
- Section 6.2.2, “Locations,” on page 98
- Section 6.2.3, “Integrity and Remediation Rules,” on page 109

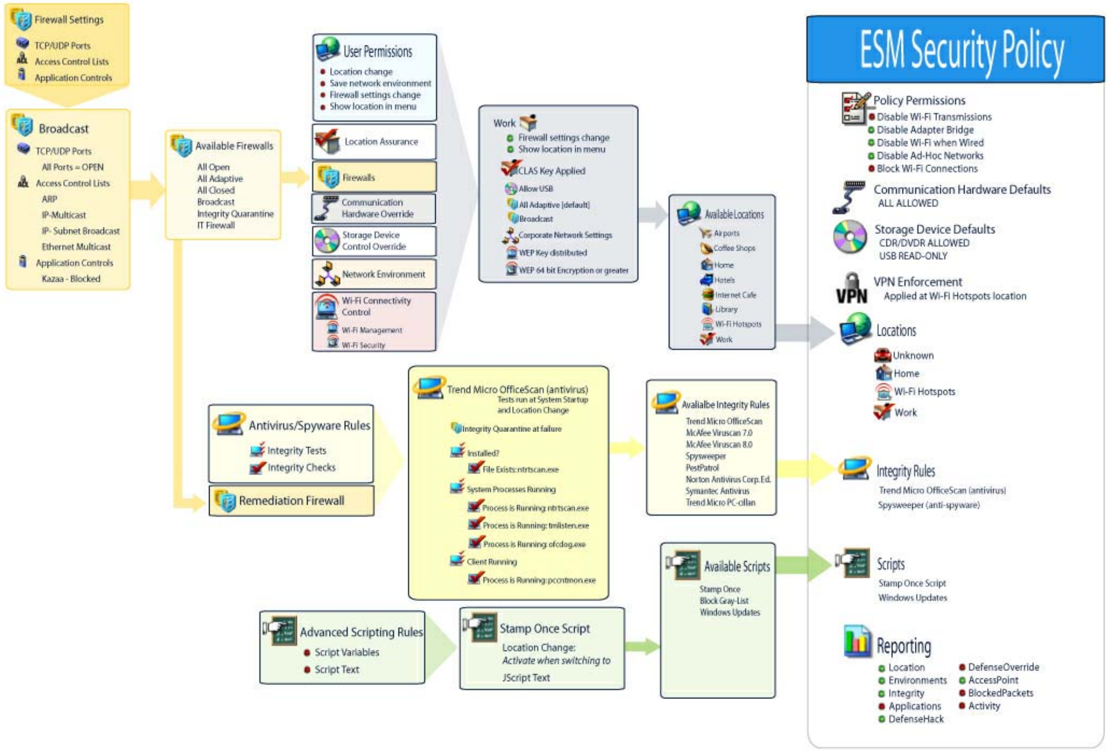
- Section 6.2.4, “Compliance Reporting,” on page 118
- Section 6.2.5, “Publishing Security Policies,” on page 121

Security policies are built by defining all the Global Settings (default behaviors), then creating and associating existing components for that policy, such as locations, firewalls and integrity rules, and finally establishing compliance reporting for the policy.

The components are created either within a dummy policy or are associated from other policies. It is assumed that for your first few policies you are creating all of the unique locations, firewall settings and integrity rules for the enterprise. These components are stored in the Management Service’s database for possible later use in other policies.

The diagram below shows the components for each level and a resulting policy taken from the selections.

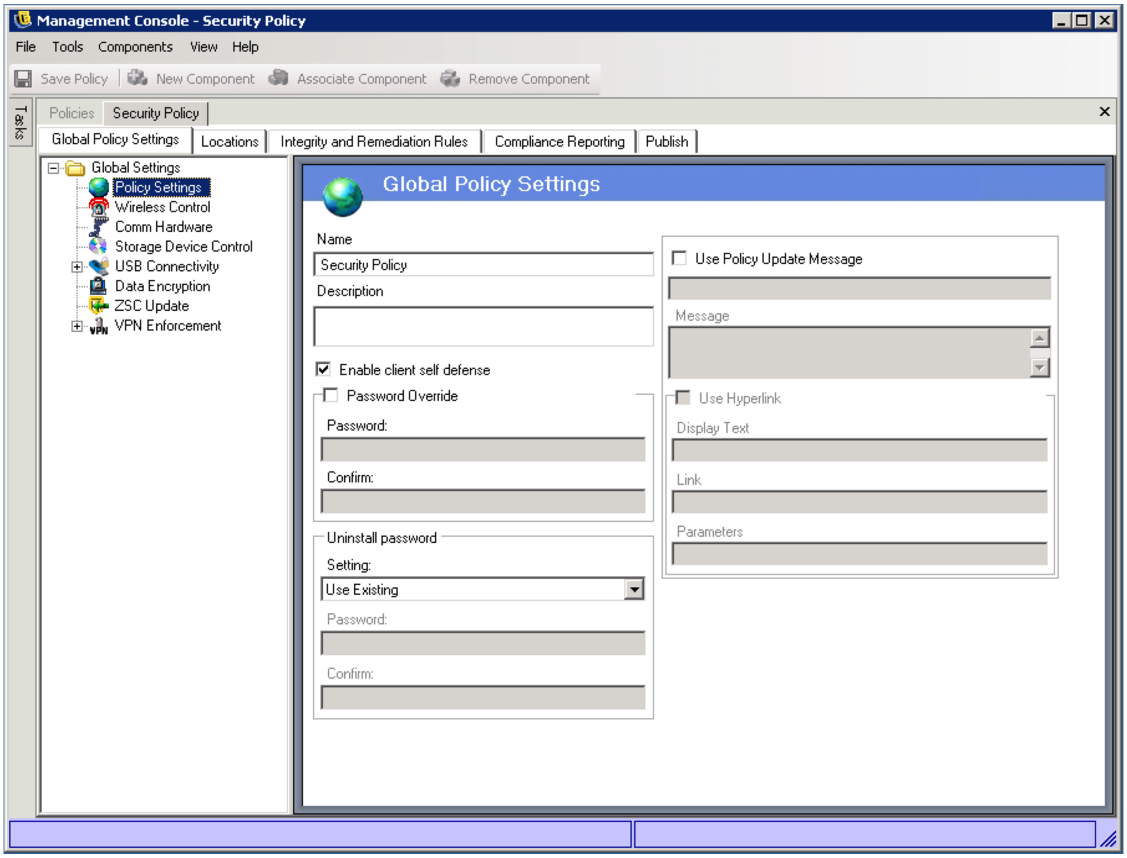
Figure 6-4 *ZENworks Endpoint Security Management Security Policy creation process*



6.2.1 Global Policy Settings

The global policy settings are applied as basic defaults for the policy. To access this control, in the Management Console, click the *Global Policy Settings* tab.

***Figure 6-5** Global Policy Settings*



Name: Security Policy

Description:

☑ Enable client self defense

☐ Password Override

Password:

Confirm:

Uninstall password

Setting: Use Existing

Password:

Confirm:

☐ Use Policy Update Message

☐ Use Hyperlink

The following sections contain more information about the settings you can configure on a global basis:

- "Policy Settings" on page 81
- "Wireless Control" on page 82
- "Communication Hardware" on page 84
- "Storage Device Control" on page 85
- "USB Connectivity" on page 88
- "Data Encryption" on page 91
- "ZSC Update" on page 94
- "VPN Enforcement" on page 95

Policy Settings

The primary global settings include:

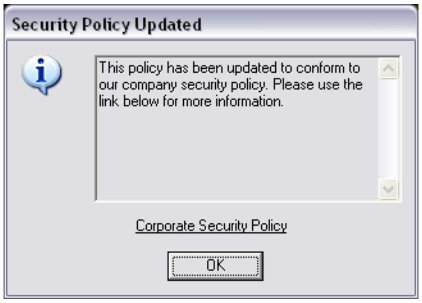
- **Name and Description:** The policy name was specified at the beginning of the policy creation process. You can edit the name or provide a description of the policy.
- **Enable client self defense:** Client Self Defense can be enabled or disabled by policy. Leaving this box checked ensures that Client Self Defense is active. Unchecking the box deactivates Client Self Defense for all endpoints using this policy.

- **Password Override:** This feature allows an administrator to set a password override that can temporarily disable the policy for a specified period of time. Check the *Password Override* box and enter the password in the provided field. Enter the password again in the confirmation field. Use this password in the Override Password Generator to generate the password key for this policy.

  WARNING: It is highly recommended that end users are not given this password, rather the Override Password Generator should be used to generate a temporary key for them.

- **Uninstall Password:** We recommend that every Endpoint Security Client be installed with an uninstall password to prevent users from uninstalling the software. This password is normally configured at installation; however, the password can be updated, enabled, or disabled via policy.
  - The default setting is Use Existing, which will not change the uninstall password.
  - Enabled is used to either activate an uninstall password or to change it. Enter the new password and confirm it.
  - Disabled is used to deactivate the uninstall password requirement.
- **Use Policy Update Message:** You can display a custom user message whenever the policy is updated. Click on the check box, then specify the message information in the provided boxes.
- **Use Hyperlink:** A hyperlink to additional information, corporate policy, or other related information can be included at the bottom of the custom message (see Section 6.3.4, "Hyperlinks," on page 124 for more information). The following is an example of the dialog box displayed to the user.

***Figure 6-6** Updated Policy Custom Message with Hyperlink*



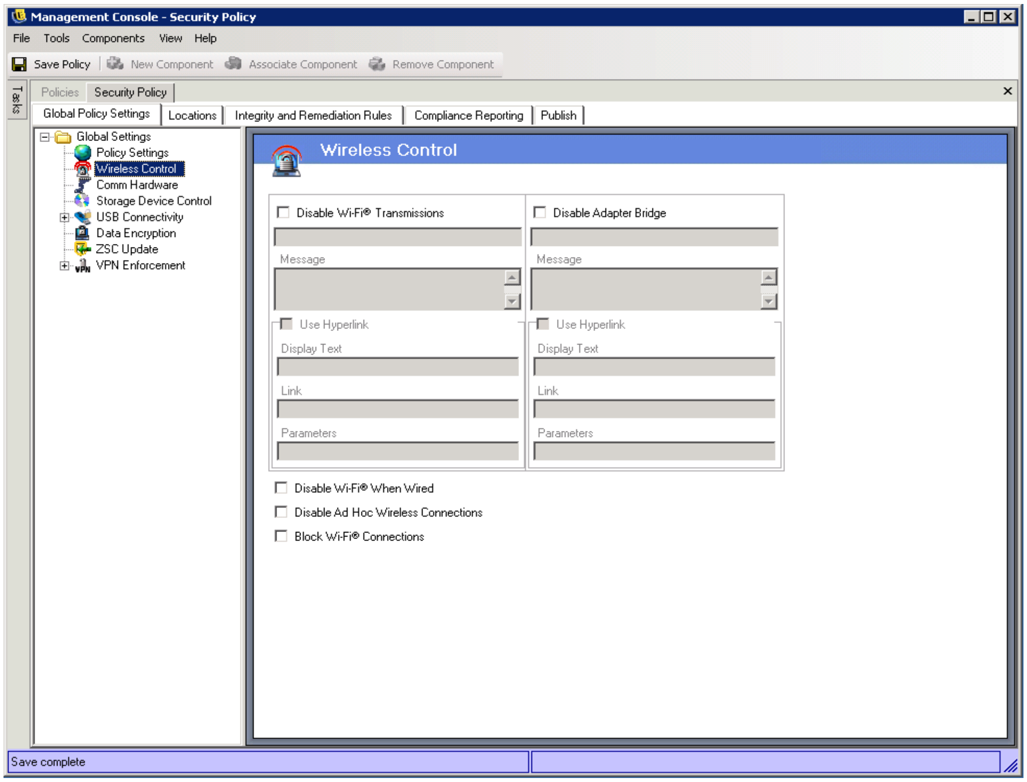
Security Policy Updated

This policy has been updated to conform to our company security policy. Please use the link below for more information.

Wireless Control

Wireless Control globally sets adapter connectivity parameters to secure both the endpoint and the network. To access this control, click the *Global Policy Settings* tab, then click the *Wireless Control* icon in the policy tree on the left.

Figure 6-7 Wireless Control Policy



☐ Disable Wi-Fi® Transmissions

☐ Disable Adapter Bridge

☐ Disable Wi-Fi® When Wired

☐ Disable Ad Hoc Wireless Connections

☐ Block Wi-Fi® Connections

Save complete

The wireless control settings include the following:

- **Disable Wi-Fi Transmissions:** This setting globally disables all Wi-Fi adapters, up to and including complete silencing of a built-in Wi-Fi radio.

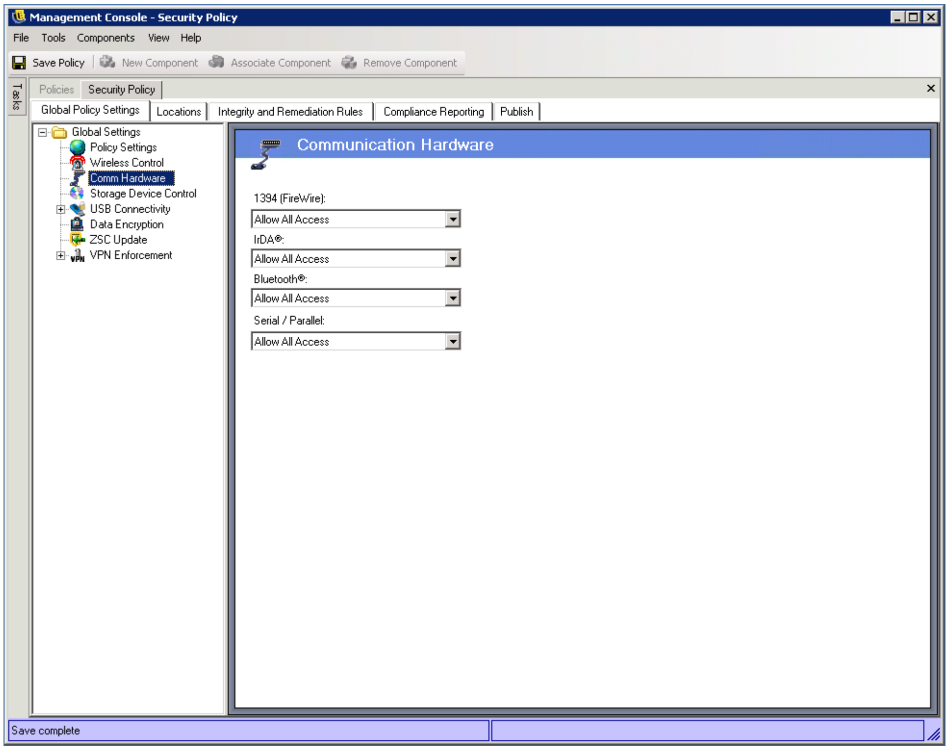
  You can choose to display a custom user message and hyperlink when the user attempts to activate a Wi-Fi connection. See Section 6.3.3, "Custom User Messages," on page 123 for more information.
- **Disable Adapter Bridge:** This setting globally disables the networking bridge functionality included with Windows XP, which allows the user to bridge multiple adapters and act as a hub on the network.

  You can choose to display a custom user message and hyperlink when the user attempts a Wi-Fi connection. See Section 6.3.3, "Custom User Messages," on page 123 for more information.
- **Disable Wi-Fi When Wired:** This setting globally disables all Wi-Fi Adapters when the user has a wired (LAN through the NIC) connection.
- **Disable AdHoc Networks:** This setting globally disables all AdHoc connectivity; thereby, enforcing Wi-Fi connectivity over a network (for example, via an access point) and restricts all peer-to-peer networking of this type.
- **Block Wi-Fi Connections:** This setting globally blocks Wi-Fi connections without silencing the Wi-Fi radio. Use this setting when you want to disable Wi-Fi connection, but want to use access points for location detection. See Section 6.2.2, "Locations," on page 98 for more information.

Communication Hardware

Communication hardware controls, by location, which hardware types are permitted a connection within this network environment.

Figure 6-8 *Communication Hardware Policy*



1394 (FireWire): Allow All Access

IrDA®: Allow All Access

Bluetooth®: Allow All Access

Serial / Parallel: Allow All Access

NOTE: You can set the communication hardware controls globally on the *Global Policy Settings* tab or for individual locations on the *Locations* tab.

To access this control:

To set the communication hardware controls on a global basis, click the *Global Policy Settings* tab, expand *Global Settings* in the tree, then click *Comm Hardware*.

or

To set the communication hardware controls for a location, click the *Locations* tab, expand the desired location in the tree, then click *Comm Hardware*. For more information about setting the communication hardware settings for a location, see "Communication Hardware" on page 100.

Select to either allow or disable the global setting for each communication hardware device listed:

- **1394 (FireWire):** Controls the FireWire access port on the endpoint.
- **IrDA:** Controls the infrared access port on the endpoint.
- **Bluetooth:** Controls the Bluetooth access port on the endpoint.
- **Serial/Parallel:** Controls serial and parallel port access on the endpoint.

Storage Device Control

Storage device controls set the default storage device settings for the policy, where all external file storage devices are either allowed to read/write files, function in a read-only state, or be fully disabled. When disabled, these devices are rendered unable to retrieve any data from the endpoint; while the hard drive and all network drives remain accessible and operational.

NOTE: You can set the storage device controls globally on the *Global Policy Settings* tab or for individual locations on the *Locations* tab.

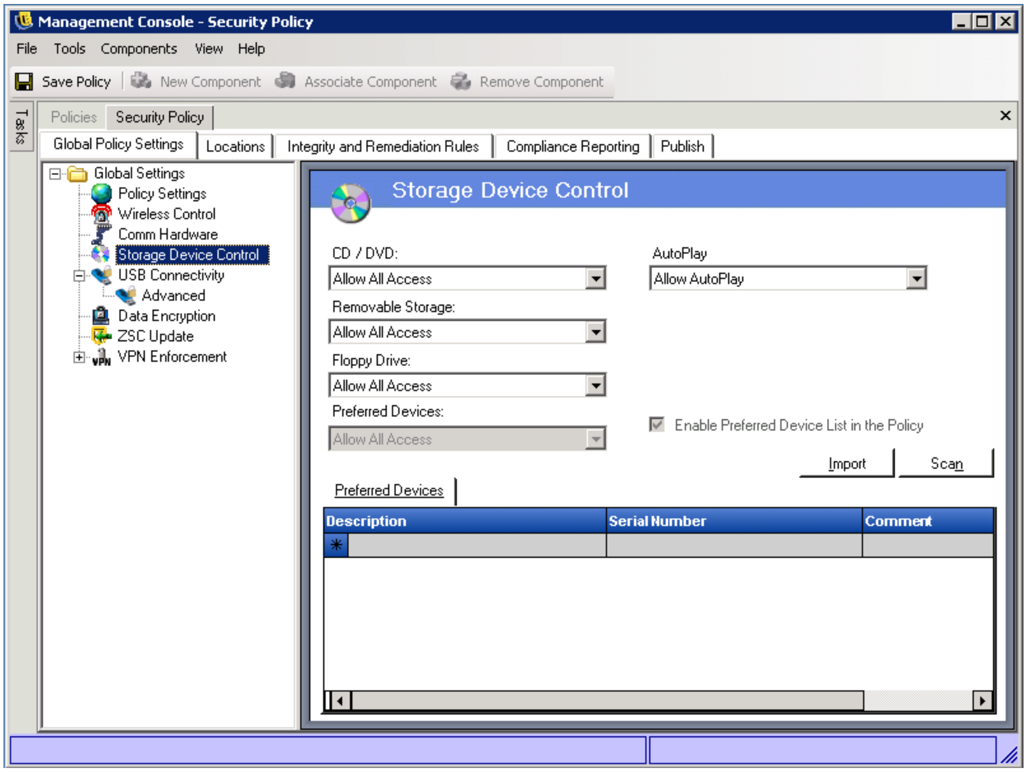
To access this control:

To set the storage device controls on a global basis, click the *Global Policy Settings* tab, expand *Global Settings* in the tree, then click *Storage Device Control*.

or

To set the storage device controls for a location, click the *Locations* tab, expand the desired location in the tree, then click *Storage Device Control*. For more information, see "Communication Hardware" on page 100.

Figure 6-9 *Global Storage Device*



CD / DVD: Allow All Access

AutoPlay: Allow AutoPlay

Removable Storage: Allow All Access

Floppy Drive: Allow All Access

Preferred Devices: Allow All Access

☑ Enable Preferred Device List in the Policy

Description	Serial Number	Comment
*		

Storage Device Control is differentiated into the following categories:

- **CD/DVD:** Controls all devices listed under *DVD/CD-ROM drives* in Windows Device Manager.
- **Removable Storage:** Controls all devices reporting as Removable storage under Disk drives in Windows Device Manager.

- **Floppy Drive:** Controls all devices listed under *Floppy disk drives* in Windows Device Manager.
- **Preferred Devices:** Allows only Removable Storage devices included in the Preferred Devices list. All other devices reporting as removable storage are not allowed. For information about adding preferred devices, see "Preferred Devices" on page 87.
- **AutoPlay:** Controls the Windows AutoPlay feature. AutoPlay performs two processes. First, it launches the AutoRun process, which looks for an autorun.inf in the root directory and executes the instructions in the file. Second, it looks for specific content (music, video, and pictures) and launches the appropriate application to display or play the content. Select one of the following options:
    - *Allow AutoPlay*: Allows the AutoPlay feature, including AutoRun.
    - *Block AutoPlay*: Blocks the AutoPlay feature, including AutoRun.
    - *Block AutoRun*: Blocks the AutoRun feature so that autorun.inf instructions are not executed. Launching of applications for music, video and pictures is not blocked.

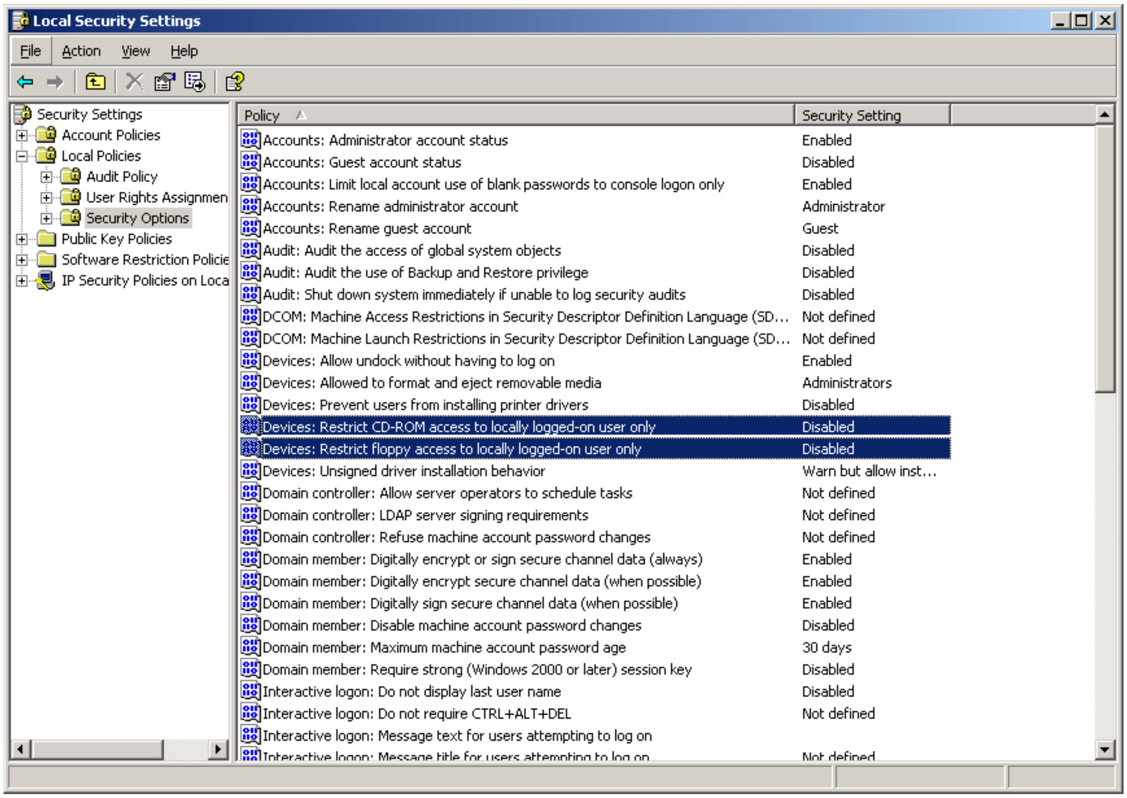
Fixed storage (hard disk drives) and network drives (when available) are always allowed.

To set the policy default for a category, select from the following options:

- **Allow All Access:** The device type is allowed by default.
- **Disable All Access:** The device type is disallowed. When users attempt to access files on a defined storage device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed
- **Read-Only Access:** The device type is set as Read-Only. When users attempt to write to the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed

NOTE: If you want to disable CD-ROM drives or floppy drives on a group of endpoints or set them as Read-Only, the Local Security Settings (passed down through a directory service group policy object) must have both *Devices: Restrict CD-ROM access to locally logged-on user only* and *Devices: Restrict floppy access to locally logged-on user only* set as *Disabled*. To verify this, open either the group policy object, or open Administrative Tools on a machine. Look in Local Security Settings - Security Options and verify both devices are disabled (see Figure 6-10). Disabled is the default.

Figure 6-10 *Verify Local Storage Device Options are set as Disabled*



Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SD...	Not defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SD...	Not defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Devices: Unsigned driver installation behavior	Warn but allow inst...
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Not defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	Not defined

Preferred Devices

Preferred Removable Storage Devices may be optionally entered into a list, permitting only the authorized devices access when the global setting is used at a location. Devices entered into this list must have a serial number.

To add a preferred device:

1. Manually enter the device information. To do so, click a field (*Description*, *Serial Number*, *Comment*) and type the information.

   or

   Scan the device information. To do so, insert the device into a USB port on the Manangement Console’s machine, then click *Scan*.

2. Select one of the following settings from the Preferred Devices list. All Removable Storage devices use the same setting:

   - **Allow All Access:** The devices in the Preferred Devices list are permitted full read/write capability. All other Removable Storage devices are disabled.
   - **Read-Only Acess:** The devices on the Preferred Devices list are permitted read-only capability. All other Removable Storage devices are disabled.

NOTE: Location-based Storage Device Control settings override the global settings. For example, you might define that at the Work location, all external storage devices are permitted, while allowing only the global default at all other locations, limiting users to the devices on the preferred list.

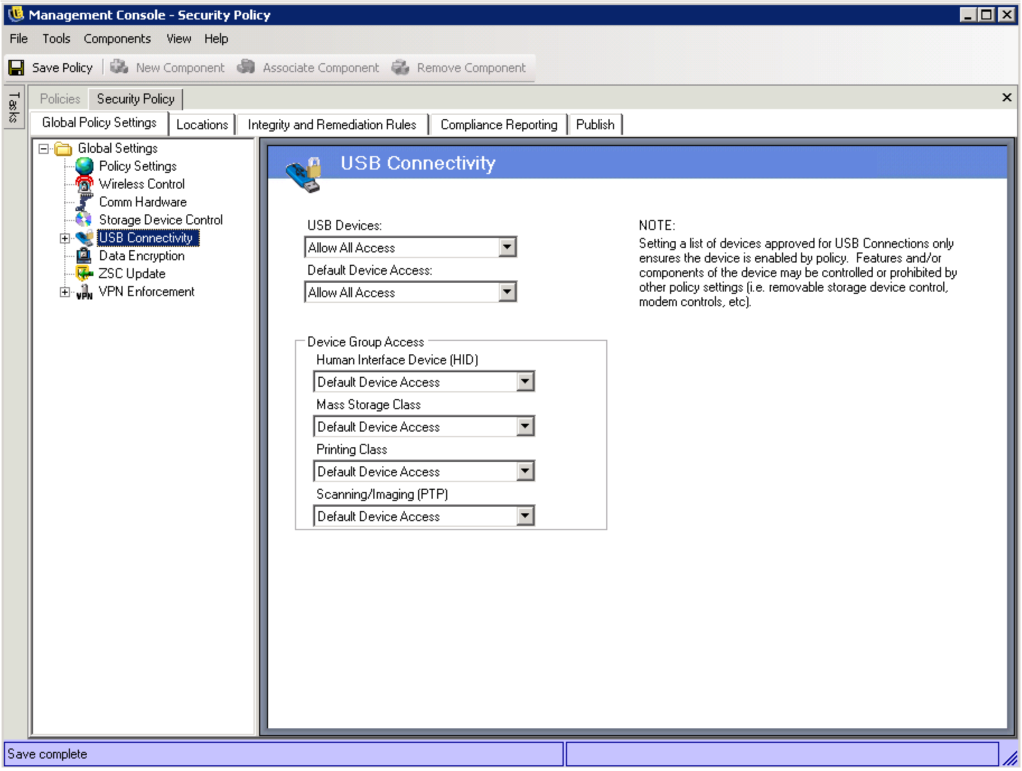
USB Connectivity

All devices that connect via the USB BUS can be allowed or denied by policy. These devices can be scanned into the policy from the USB Device Inventory report or by scanning all devices currently connected to a machine. These devices can be filtered based on manufacturer, product name, serial numbers, type, and so forth.

For support purposes, the administrator can configure the policy to accept a set of devices, either by manufacturer type, (for example, all HP devices are allowed), or by product type (all USB-human interface devices [mouse and keyboard] are allowed). Additionally, individual devices can be permitted to prevent non-supported devices from being introduced into the network (for example, no printers are allowed except for this one).

To access this control, click the *Global Policy Settings* tab, then click *USB Connectivity* in the policy tree on the left.

Figure 6-11 *USB Connectivity page.*



USB Devices: Allow All Access

Default Device Access: Allow All Access

Device Group Access

Human Interface Device (HID): Default Device Access

Mass Storage Class: Default Device Access

Printing Class: Default Device Access

Scanning/Imaging (PTP): Default Device Access

NOTE:
Setting a list of devices approved for USB Connections only ensures the device is enabled by policy. Features and/or components of the device may be controlled or prohibited by other policy settings (i.e. removable storage device control, modem controls, etc).

Save complete

Access is first evaluated based on whether the bus is active or not. This is determined by the *USB Devices* setting. If this setting is set to *Disable All Access*, the device is disabled and evaluation stops. If this setting is set to *Allow All Access*, the client continues the evaluation and set looking for filter matches. As with many other fields in the ZENworks Management Console, when being set on a location, the *USB Devices* value can also be set to *Apply Global Settings* and the global value of this field will be used instead.

The client gathers the filters that are applied from the policy, based on the location and global settings.

The client will then group the filters based on access into the following groups:

- **Always Block:** Always block the device. This setting cannot be overridden.
- **Always Allow:** Always allow access unless the device matches an *Always Block* filter.
- **Block:** Block access unless the device matches an *Always Allow* filter.
- **Allow:** Allow access unless the device matches an *Always Block* or a *Block* filter.
- **Default Device Access:** Give the device the same access level as *Default Device Access* if no other match is found.

A device is evaluated against each group in the above order (first the *Always Block* group, followed by *Always Allow*, and so forth). When a device matches at least one filter in a group, the device's access is set to that level and evaluation stops. If the device is evaluated against all filters, and no match is found, the *Default Device Access* level is applied.

Device Access set in the *Device Group Access* area is considered along with all other filters being used at that location. This is done by generating matching filters for each of the grouping when the policy is published to the client. These filters are as follows:

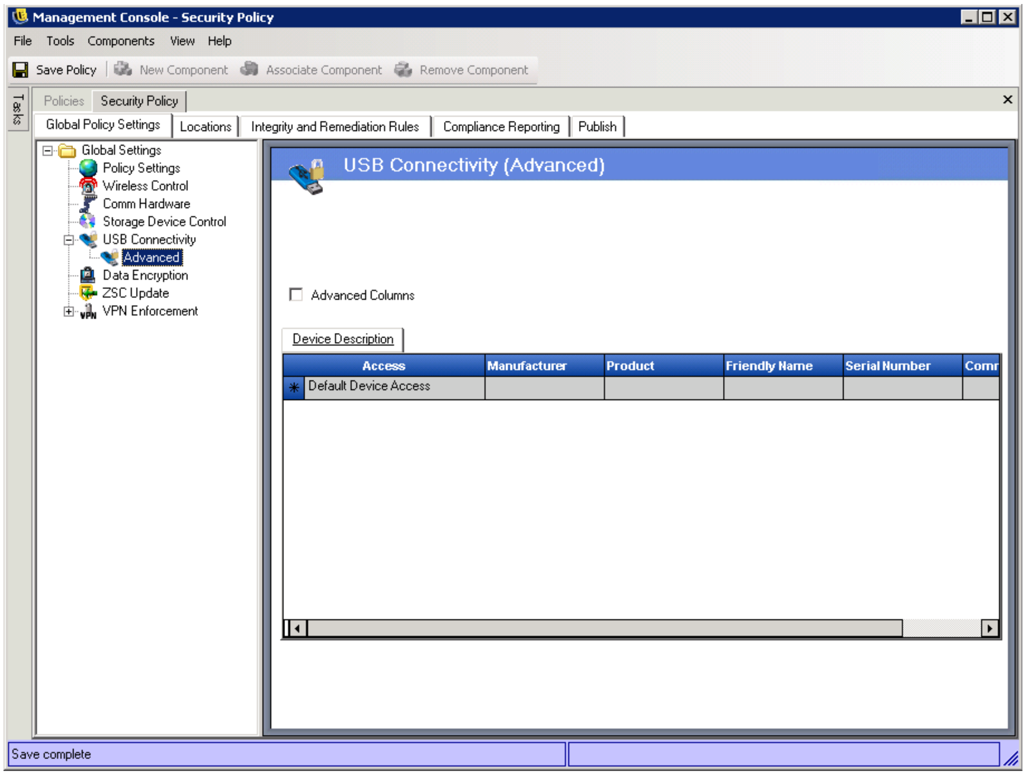
Device Group Access:	Filter:
Human Interface Device(HID)	"Device Class" is equal to 3.
Mass Storage Class	"Device Class" is equal to 8.
Printing Class	"Device Class" is equal to 7.
Scanning/Imaging (PTP)	"Device Class" is equal to 6.

Advanced

In most situations, the four device groups listed on the USB Connectivity page (Human Interface Device, Mass Storage Class, Printing Class, and Scanning/Imaging) are sufficient to allow or deny access to most USB devices. If you have devices that do not register in one of these groups, you can configure settings on the USB Connectivity Advanced page. You can also use the settings on the Advanced page to provide whitelist access to certain devices even though they might be denied access because of the settings on the USB Connectivity page.

To access the Advanced USB Connectivity options, click the plus sign next to *USB Connectivity* in the *Global Settings* tree, then click *Advanced*. You can use the USB Device Audit report as a means of getting all the information you could potentially use on the USB Connectivity Control Advanced page.

Figure 6-12 USB Connectivity Advanced page.



To add a device to the list, fill in the following fields:

- **Access:** Select an access level:
  - **Always Block:** Always block the device. This setting cannot be overridden.
  - **Always Allow:** Always allow access unless the device matches an *Always Block* filter.
  - **Block:** Block access unless the device matches an *Always Allow* filter.
  - **Allow:** Allow access unless the device matches an *Always Block* or a *Block* filter.
  - **Default Device Access:** Give the device the same access level as *Default Device Access* if no other match is found.
- **Manufacturer:** Click the *Manufacturer* column then type the name of the manufacturer you want to include in the filter (Canon, for example).
- **Product:** Click the *Product* column then type the name of the product you want to include in the filter.
- **Friendly Name:** Click the *Friendly Name* column then type the friendly name of the device you want to include in the filter.
- **Serial Number:** Click the *Serial Number* column then type the serial number of the device you want to include in the filter.
- **Comment:** Click the *Comment* column then type the comment you want to include in the filter (Canon, for example).

You can click the *Advanced Columns* box to add the following columns: *USB Version*, *Device Class, Device Sub-Class, Device Protocol, Vendor ID, Product ID, BCD Device, O/S Device ID*, and *O/S Device Class*.

A device makes available a set of attributes to the OS. These attributes are matched by the client to the fields required by a filter. All fields in the filter must match an attribute provided by the device in order to have a match. If the device does not provide an attribute or field that is required by the filter, that filter fails to match.

For example, suppose a device provides the following attributes: Manufacture: Acme Class: 8, Serial Number: "1234".

The filter: Class == 8 would match this device. The filter: Product == "Acme" would not match because the device did not provide a Product attribute to the OS.

The following fields are sub-string matched: Manufacturer, Product, and Friendly Name. All other fields are exact matches.

As a matter of interest, USB serial number(SN) field by spec. is only unique when considered when specifying the following fields along with the SN: USB Version, Vendor ID, Production ID, and BCD Device.

Current valid values for USB version in decimal are: 512 - USB 2.0, 272 - USB 1.1, 256 - USB 1.0.

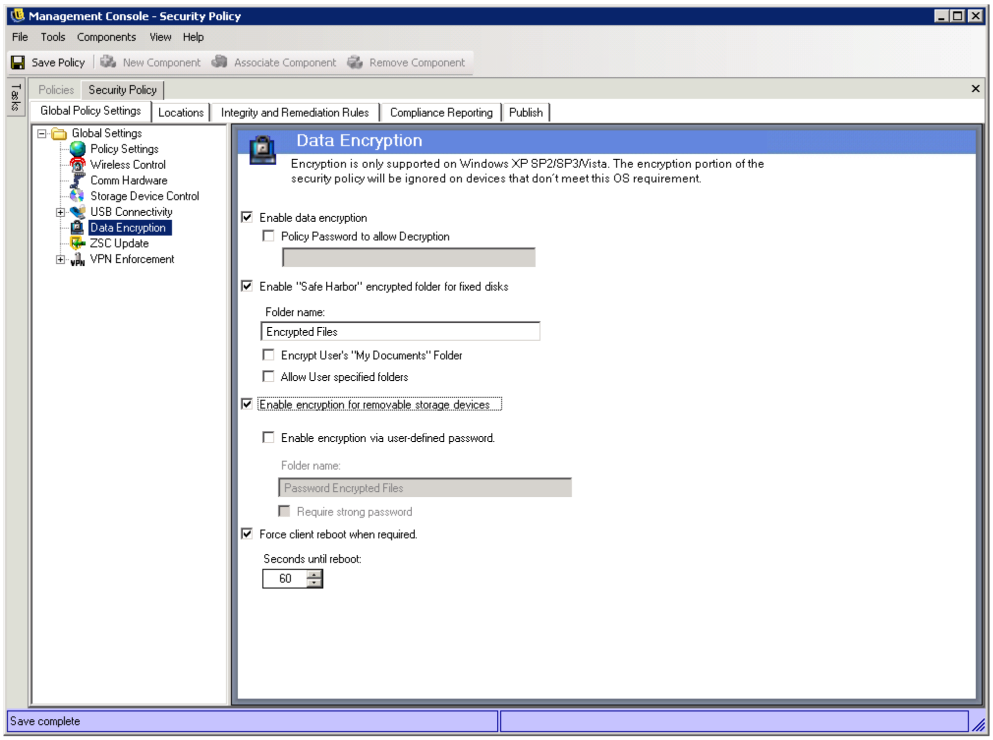
Data Encryption

Data Encryption determines whether file encryption is enforced on the endpoint and what type of encryption is available. Data can be encrypted to permit file sharing (with password protection) or can set encrypted data to be read-only on computers running the Storage Encryption Solution.

NOTE: Encryption is supported only on Windows XP SP2. The encryption portion of the security policy is ignored on devices that do not meet this OS requirement.

To access this control, click the *Global Policy Settings* tab, then click *Data Encryption* in the policy tree on the left.

Figure 6-13 *Data Encryption controls*


Management Console - Security Policy
File Tools Components View Help
Save Policy New Component Associate Component Remove Component
Tasks
Policies Security Policy
Global Policy Settings Locations Integrity and Remediation Rules Compliance Reporting Publish
Global Settings
Policy Settings
Wireless Control
Comm Hardware
Storage Device Control
USB Connectivity
Data Encryption
ZSC Update
VPN Enforcement

Data Encryption

Encryption is only supported on Windows XP SP2/SP3/Vista. The encryption portion of the security policy will be ignored on devices that don't meet this OS requirement.

☑ Enable data encryption

☐ Policy Password to allow Decryption

☑ Enable "Safe Harbor" encrypted folder for fixed disks

Folder name: Encrypted Files

☐ Encrypt User's "My Documents" Folder

☐ Allow User specified folders

☑ Enable encryption for removable storage devices

☐ Enable encryption via user-defined password.

Folder name: Password Encrypted Files

☐ Require strong password

☑ Force client reboot when required.

Seconds until reboot: 60

Save complete

To activate the individual controls, click the *Enable Data Encryption* check box.

NOTE: Encryption keys are distributed to all machines that receive policies from the Policy Distribution Service, regardless of whether data encryption is activated or not. However, this control instructs the Endpoint Security Client to activate its encryption drivers, which allows users to read files sent to them without requiring the File Decryption Utility. See Section 9.1, "Using the ZENworks File Decryption Utility," on page 203 for more details.

Determine what levels of encryption are permitted by this policy:

- **Policy password to allow decryption:** Entering a password here to require all users using this policy to enter this password prior to decrypting any encrypted files stored in their Safe Harbor folders.

  This is an optional setting, leave blank to not require the password.

- **Enable "Safe Harbor" encrypted folder for fixed disks:** Generates a folder at the root of all volumes on the endpoint, named `Encryption Protected Files`. All files placed in this folder are encrypted and managed by the Endpoint Security Client. Data placed in this folder is automatically encrypted and can only be accessed by authorized users on this machine.

  The folder name can be changed by clicking in the *Folder Name* field, selecting the current text, and entering the name you desire.

  - **Encrypt User's "My Documents" Folder:** Select this option to encrypt all files in the user's My Documents folder. As with the Safe Harbor folder, data placed in this folder is automatically encrypted and can only be accessed by authorized users on this machine.

  - **Allow user specified folders:** Select this option to allow users to select which folders on their computer are encrypted. This is for local folders only; no removable storage devices nor network drives can be encrypted.

WARNING: Before disabling data encryption, ensure that all data stored in these folders has been extracted by the user and stored in another location.

- **Enable encryption for removable storage devices:** All data written to removable storage devices from an endpoint protected by this policy is encrypted. Users with this policy on their machines are able to read the data; therefore, file sharing via removable storage device within a policy group is available. Users outside this policy group are not able to read the files encrypted on the drive, and will only be able to access files within the Password Encrypted Files folder (if activated) with a provided password.
  - **Enable encryption via user-defined password:** This setting gives the user the ability to store files in a Password Encrypted Files folder on the removable storage device (this folder will be generated automatically when this setting is applied).

    When a user adds files to this folder, the files are encrypted with a password that the user supplies. The user can then access the files from any device that is not running the Security client. To decrypt the files, the user needs the ZENworks File Decryption utility and the encryption password. You must supply this utility to the user; it is not part of the Security client (see Section 9.1, “Using the ZENworks File Decryption Utility,” on page 203).

    For example, assume that a user is working on encrypted files at work. The user wants to take the files home to work on them, but the home computer does not have the Security client installed. The user copies the files to the Password Encrypted Files folder on a USB thumb drive, takes the files home, then accesses them using the ZENworks File Decryption utility you provided.

    If desired, you can change the default folder name (Password Encrypted Files) to another name.
  - **Require strong password:** This setting forces the user to set a strong password for the Password Encrypted Files folder. A strong password requires the following:
    - seven or more characters
    - at least one of each of the four types of characters:
      - uppercase letters from A to Z
      - lowercase letters from a to z
      - numbers from 0 to 9
      - at least one special character ~!@#$%^&*()+{}[]:;<>?,./

    For example: y9G@wb?

WARNING: Before disabling data encryption, ensure that all data stored on removable storage devices has been extracted by the user and stored in another location.

- **Force client reboot when required:** When encryption is added to a policy, it does not become active until the endpoint is rebooted. This setting forces the required reboot by displaying a countdown timer, warning the user that the machine will reboot in the specified number of seconds. The user has that amount of time to save work before the machine reboots.

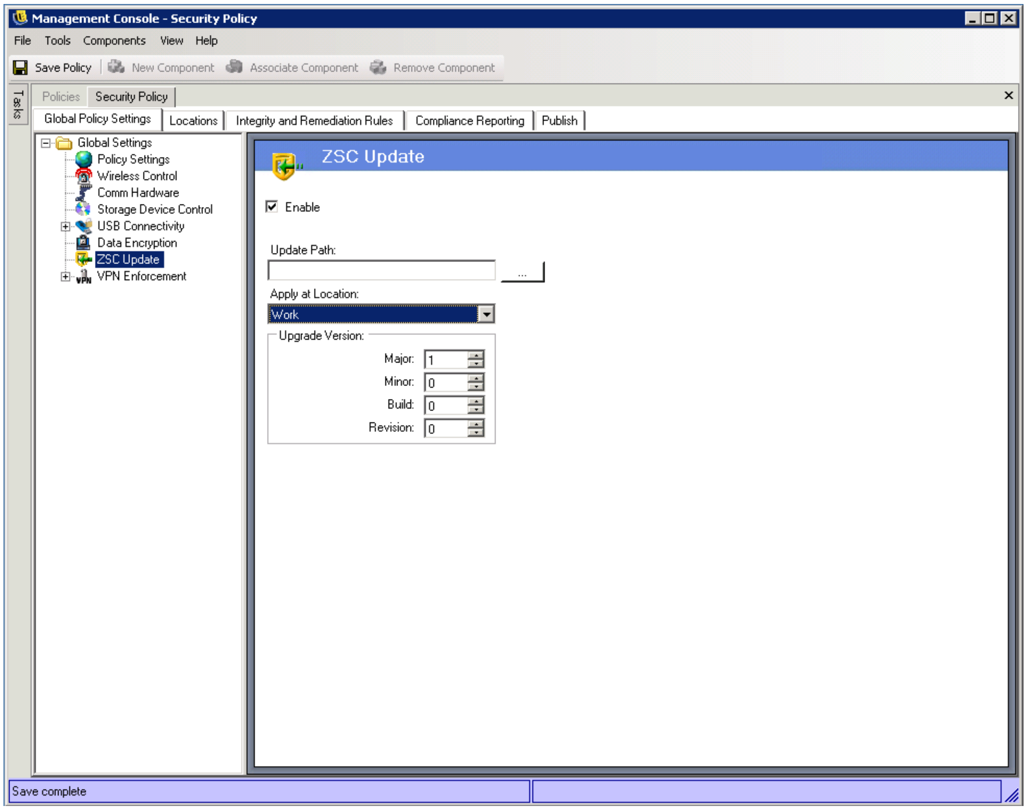
  Reboots are required when encryption is first activated in a policy, and again when either “Safe Harbor” or removable storage encryption is activated (if activated separately from encryption activation). For example, when an encryption policy is applied for the first time, two reboots are required: one reboot to initialize the drivers and another reboot to put any safe harbors into encryption. If additional safe harbors are subsequently selected after the policy has been applied, only one reboot is required to put the safe harbor into policy.

ZSC Update

Patches to repair any minor defects in the Endpoint Security Client are made available with regular ZENworks Endpoint Security Management updates. Rather than providing a new installer, which needs to be distributed through MSI to all endpoints, ZENworks Security Client Update allows the administrator to dedicate a zone on the network that distributes update patches to end users when they associate to that network environment.

To access this control, click the *Global Policy Settings* tab, then click *ZSC Update* in the policy tree on the left.

Figure 6-14 *ZSC Update*



☑ Enable

Update Path:

Apply at Location: Work

Upgrade Version:

Major: 1
Minor: 0
Build: 0
Revision: 0

Save complete

To facilitate simple and secure distribution of these patches to all Endpoint Security Client users:

1. Check Enable to activate the screen and the rule.

2. Specify the location where the Endpoint Security Client looks for the updates. Due to the recommendations in the next step, the location associated with the enterprise environment (i.e.: the "Work" location) is the recommended candidate.
3. Enter the URI where the patch has been stored. This needs to point to the patch file, which can be either the `setup.exe` file for the Endpoint Security Client, or an MSI file created from the `.exe` file). For security purposes, it is recommended that these files be stored on a secure server behind the corporate firewall.
4. Enter the version information for this file in the provided fields. Version information is found by installing the Endpoint Security Client and opening the About screen (see the *ZENworks Endpoint Security Management Installation Guide* for details). The version number for `STEngine.exe` is the version number you want to use in the fields.

Each time the user enters the assigned location, the Endpoint Security Client checks the URI for an update that matches that version number. If an update is available, the Endpoint Security Client downloads and installs it.

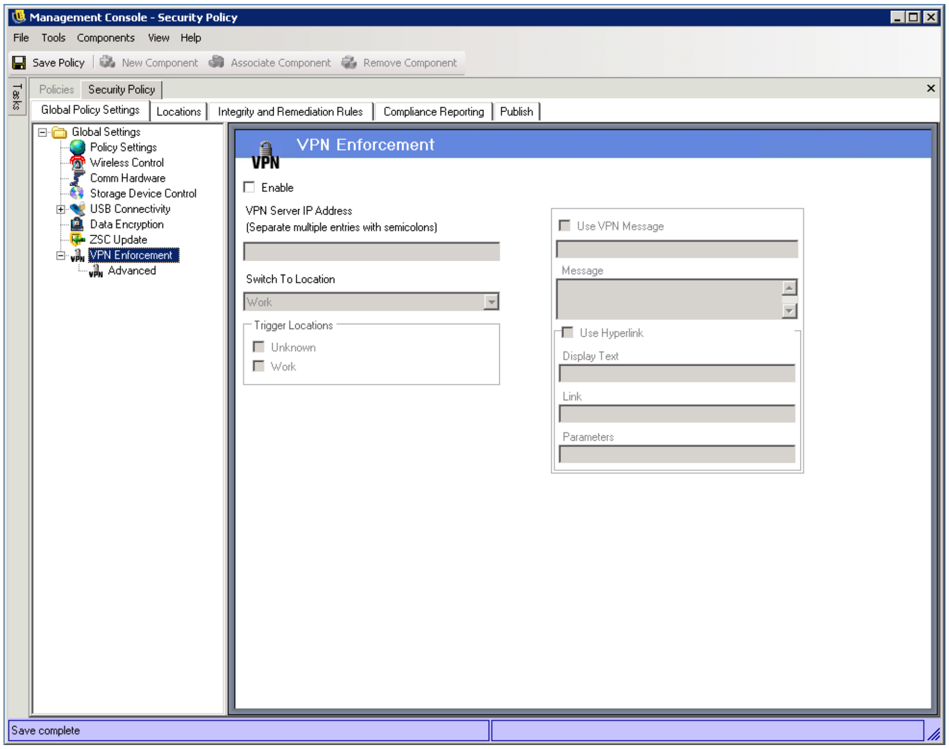
VPN Enforcement

This rule enforces the use of either an SSL or a client-based VPN (Virtual Private Network). This rule is typically applied at wireless hotspots, allowing the user to associate and connect to the public network, at which time the rule attempts to make the VPN connection, then switches the user to a defined location and firewall setting. All parameters are at the discretion of the administrator. All parameters override existing policy settings. The VPN-Enforcement component requires the user be connected to a network prior to launching.

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for UWS security policies.

To access this control, click the *Global Policy Settings* tab, then click *VPN Enforcement* in the policy tree on the left.

Figure 6-15 *Basic VPN Enforcement*



□ Enable

VPN Server IP Address
(Separate multiple entries with semicolons)

Switch To Location: Work

Trigger Locations
□ Unknown
□ Work

□ Use VPN Message

Message

□ Use Hyperlink

Display Text

Link

Parameters

Save complete

To use the VPN Enforcement rule, at least two locations must exist.

To add VPN enforcement to a new or existing security policy:

1. Select *Enable* to activate the screen and the rule.
2. Specify the IP addresses for the VPN Server in the provided field. If multiple addresses are specified, separate each with a semi-colon (for example: 10.64.123.5;66.744.82.36).
3. Select the Switch To Location from the drop-down list. The Endpoint Security Client switches to this location after the VPN authenticates.

   The Switch To location is the location the Endpoint Security Client switches to when the VPN is activated. It is recommended that this location contain some restrictions, and only a single restrictive firewall setting as its default.

   The *All-Closed* firewall setting, which closes all TCP/UDP ports, is recommend for strict VPN enforcement. This setting prevents any unauthorized networking, while the VPN IP address acts as an ACL to the VPN server, and permits network connectivity.
4. Select the Trigger locations where the VPN enforcement rule is applied. For strict VPN enforcement, it is recommended the default Unknown location be used for this policy. After the network has authenticated, the VPN rule activates and switches to the assigned Switch To Location.

   NOTE: The location switch occurs before the VPN connection, after the network has authenticated.
5. Enter a Custom User Message to display when the VPN has authenticated to the network. For non-client VPNs, this should be suffiClient.

For VPNs with a client, include a hyperlink that points to the VPN Client.

Example: `C:\Program Files\Cisco Systems\VPN Client\ipsecdialer.exe`

This link launches the application, but the user stills need to log in. A switch can be entered into the Parameters field, or a batch file could be created and pointed to, rather than the client executable).

NOTE: VPN clients that generate virtual adapters (for example, Cisco Systems* VPN Client 4.0) display the: "Policy Has Been Updated" message. The Policy has not been updated, the Endpoint Security Client is simply comparing the virtual adapter to any adapter restrictions in the current policy.

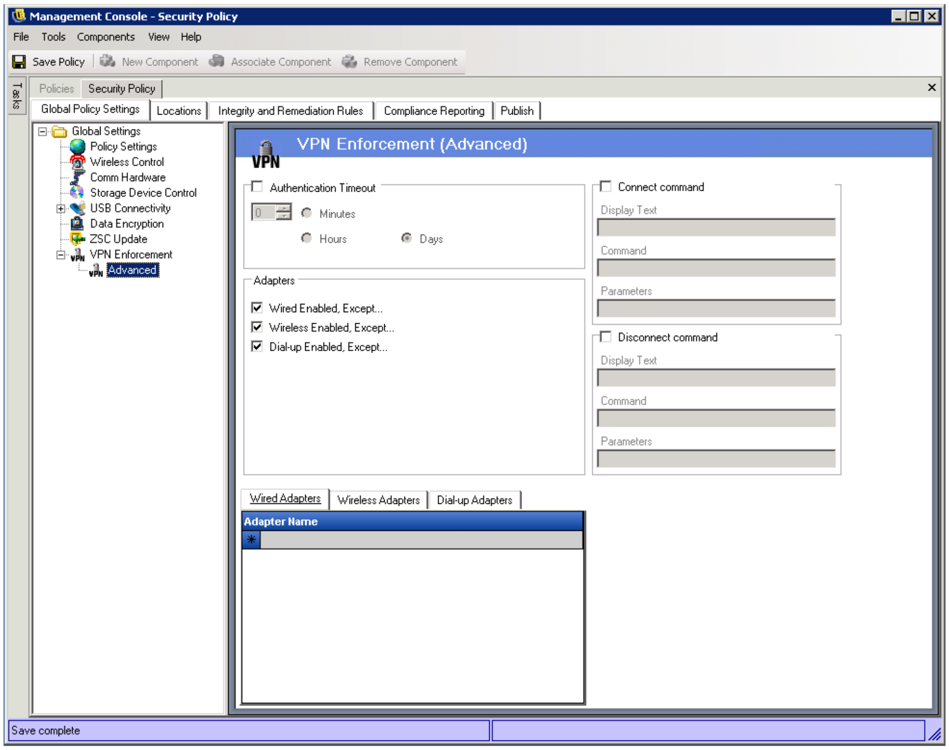
The standard VPN Enforcement settings described above make VPN connectivity an option. Users are granted connectivity to the current network whether they launch their VPN or not. For stricter enforcement, see Advanced VPN Settings below.

Advanced VPN Settings

Advanced VPN controls are used to set Authentication Timeouts to secure against VPN failure, connect commands for client-based VPNs, and use Adapter controls to control the adapters permitted VPN access.

To access this control, click the *Global Policy Settings* tab, click the “+” symbol next to *VPN Enforcement*, then click `Advanced` in the policy tree on the left.

Figure 6-16 *Advanced VPN Enforcement*



VPN Enforcement (Advanced)

☐ Authentication Timeout

0 ○ Minutes

○ Hours ● Days

Adapters

☑ Wired Enabled, Except...

☑ Wireless Enabled, Except...

☑ Dial-up Enabled, Except...

☐ Connect command

Display Text

Command

Parameters

☐ Disconnect command

Display Text

Command

Parameters

Wired Adapters | Wireless Adapters | Dial-up Adapters

Adapter Name
*

Save complete

The following advanced VPN enforcement settings can be configured:

Authentication Timeout: Administrators can place the endpoint in a secured firewall setting (the firewall *Switch To Location* setting) to secure against any failure of VPN connectivity. The *Authentication Timeout* is the amount of time the Endpoint Security Client waits to gain authentication to the VPN server. It is recommended that this parameter be set above 1 minute to allow authentication over slower connections.

Connect/Disconnect Commands: When using the Authentication timer, the *Connect* and *Disconnect* commands control client-based VPN activation. Specify the location of the VPN client and the required switches in the *Parameters* fields. The Disconnect command is optional, and provides for VPN clients that require that the user disconnects before logging off of the network.

NOTE: VPN clients that generate virtual adapters (for example, Cisco Systems VPN Client 4.0) display the: "Policy Has Been Updated" message, and may switch away from the current location temporarily. The Policy has not been updated, the Endpoint Security Client is simply comparing the virtual adapter to any adapter restrictions in the current policy. It is recommended that when running VPN clients of this type that the Disconnect command hyperlink not be used.

Adapters: This is essentially a mini Adapter policy specific to the VPN Enforcement.

If an adapter is checked (changing it to Enabled, Except), those adapters (Wireless being specific to card type) are permitted connectivity to the VPN.

Adapters entered into the exception lists below, are denied connectivity to the VPN, while all others of that type will be given connectivity.

If an adapter is not checked (Disabled, Except), then only the adapters entered into the exception list are permitted to connect to the VPN; all others are denied connectivity.

This control can be used for adapters incompatible to the VPN, for example, or adapters not supported by the IT department.

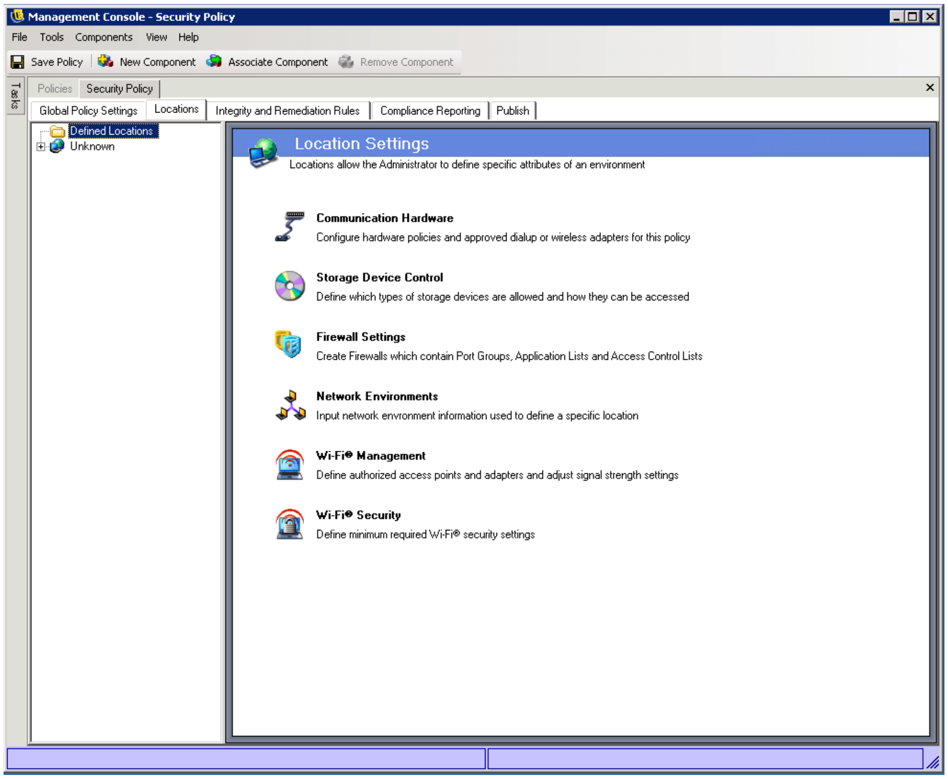
This rule overrides the adapter policy set for the switch-to location.

6.2.2 Locations

Locations are rule-groups assigned to network environments. These environments can be set in the policy (see Section 6.3.6, “Network Environments,” on page 126), or by the user, when permitted. Each location can be given unique security settings, denying access to certain kinds of networking and hardware in more hostile network environments, and granting broader access within trusted environments.

To access Location controls, click the *Locations* tab.

Figure 6-17 *Location Settings*



Location Settings

Locations allow the Administrator to define specific attributes of an environment

Communication Hardware
Configure hardware policies and approved dialup or wireless adapters for this policy

Storage Device Control
Define which types of storage devices are allowed and how they can be accessed

Firewall Settings
Create Firewalls which contain Port Groups, Application Lists and Access Control Lists

Network Environments
Input network envronment information used to define a specific location

Wi-Fi® Management
Define authorized access points and adapters and adjust signal strength settings

Wi-Fi® Security
Define minimum required Wi-Fi® security settings

The following sections contain more information:

- "About Locations" on page 99
- "Communication Hardware" on page 100
- "Storage Device Control" on page 102
- "Wi-Fi Management" on page 104
- "Wi-Fi Security" on page 108

About Locations

The following types of locations can be configured:

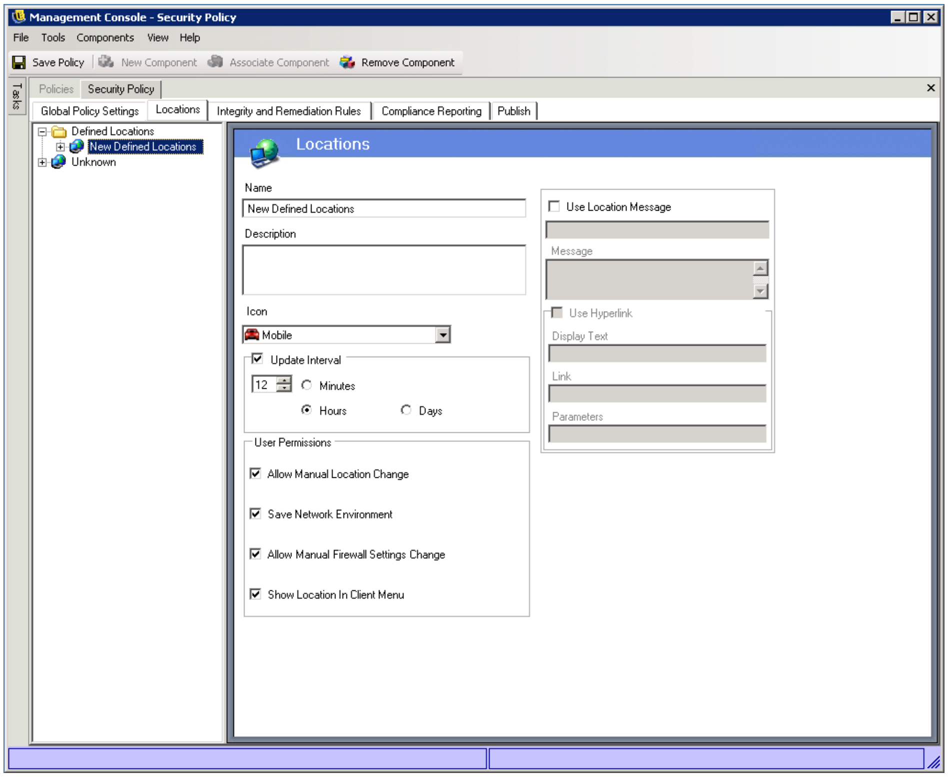
The Unknown Location: All policies have a default Unknown location. This is the location the Endpoint Security Client switches users to when they leave a known network environment. This Unknown location is unique for each policy and is not available as a shared component. Network Environments cannot be set nor saved for this location.

To access the Unknown Location controls, click the *Locations* tab, then click the *Unknown* location in the policy tree on the left.

Defined Locations: Defined locations can be created for the policy, or existing locations (those created for other policies) can be associated.

To create a new location:

1 Click *Defined Locations*, then click the *New Component* button on the toolbar.



Name: New Defined Locations

Description:

Icon: Mobile

☑ Update Interval

12 ○ Minutes ● Hours ○ Days

User Permissions

☑ Allow Manual Location Change

☑ Save Network Environment

☑ Allow Manual Firewall Settings Change

☑ Show Location In Client Menu

☐ Use Location Message

Message

☐ Use Hyperlink

Display Text

Link

Parameters

2 Name the location and provide a description.

3 Define the location settings (see below).

4 Click *Save Policy*.

To associate an existing location:

1 Click *Defined Locations*, then click the *Associate Component* button on the toolbar.

2 Select the desired locations from the list.

3 Edit the settings, if desired.

NOTE: Changing the settings in a shared component will affect all other instances of this same component. Use the *Show Usage* command to view all other policies associated with this component.

4 Click *Save Policy*.

It is recommended that multiple defined locations (beyond simple Work and Unknown locations) be defined in the policy to provide users with varying security permissions when they connect outside the enterprise firewall. Keeping the location names simple (for example, Coffee Shops, Airports, Home) and providing a visual cue through the location's Taskbar icon, which helps users easily switch to the appropriate security settings required for each network environment.

Communication Hardware

Communication hardware controls, by location, which hardware types are permitted a connection within this network environment.

NOTE: You can set the communication hardware controls globally on the *Global Policy Settings* tab or for individual locations on the *Locations* tab.

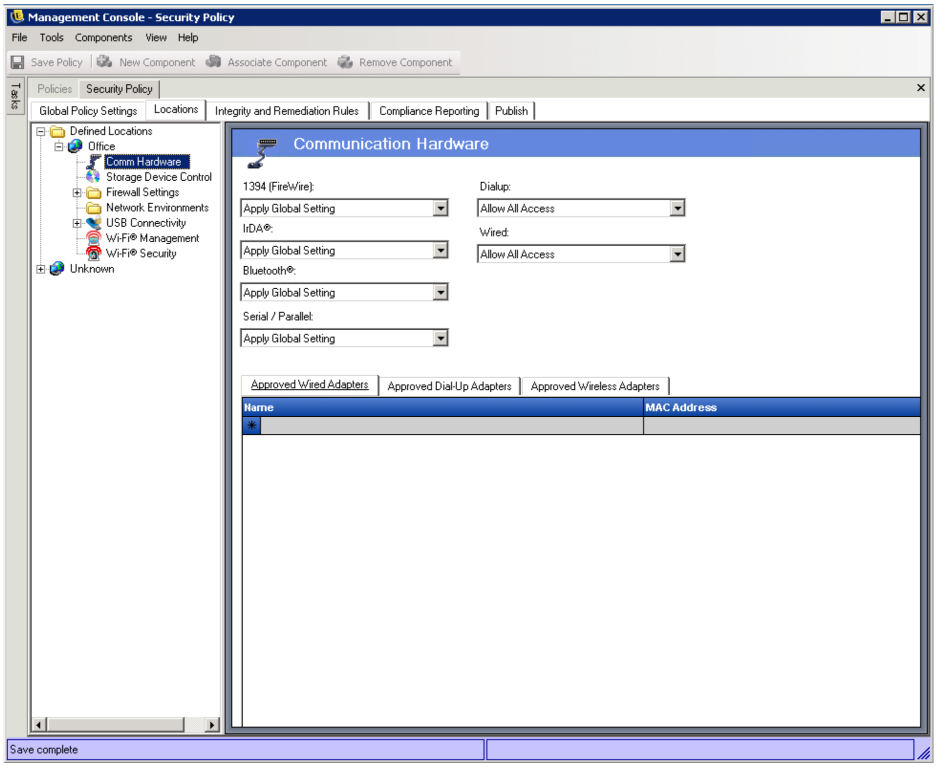
To access this control:

To set the communication hardware controls for a location, click the *Locations* tab, expand the desired location in the tree, then click *Comm Hardware*.

or

To set the communication hardware controls on a global basis, click the *Global Policy Settings* tab, expand *Global Settings* in the tree, then click *Comm Hardware*. For more information, see "Communication Hardware" on page 84.

Figure 6-18 *Location Communication Hardware Control*



1394 (FireWire): Apply Global Setting

IrDA®: Apply Global Setting

Bluetooth®: Apply Global Setting

Serial / Parallel: Apply Global Setting

Dialup: Allow All Access

Wired: Allow All Access

Name	MAC Address
*	

Save complete

To configure the settings:

1. For each communication hardware type listed below, select *Apply Global Settings*, *Allow All Access*, or *Disable All Access*:
   - **1394 (FireWire):** Controls the FireWire access port on the endpoint.
   - **IrDA:** Controls the infrared access port on the endpoint.
   - **Bluetooth:** Controls the Bluetooth access port on the endpoint.
   - **Serial/Parallel:** Controls serial and parallel port access on the endpoint.

- **Dialup:** Controls modem connectivity by location. This option is not available when configuring communication hardware settings on a global basis using the *Global Policy Settings* tab. If you want to limit access to specific modems, set this option to *Allow All Access* and then add the approved modems to the *Approved Dial-Up Adapters* list.
- **Wired:** Controls LAN card connectivity by location. This option is not available when configuring communication hardware settings on a global basis using the *Global Policy Settings* tab. If you want to limit access to specific wired adapters, set this option to *All All Access* and then add the approved adapters to the *Approved Wired Adapters* list.

2 (Optional) If you selected *Allow All Access* for the *Dialup* or *Wired* settings and you want to limit the adapters that are allowed, add the approved adapters to the appropriate list (*Approved Wired Adapters* or *Approved Dialup Adapters*.

Partial adapter names are permitted. Adapter names are limited to 50 characters and are case sensitive. Only the adapters included in the list are allowed; all other adapters are blocked.

3 (Optional) If you have enabled Wi-Fi (see "Wi-Fi Management" on page 104) and you want to limit the wireless adapters that are allowed, add the approved adapters to the *Approved Wireless Adapters* list.

Partial adapter names are permitted. Adapter names are limited to 50 characters and are case sensitive. Only the adapters included in the list are allowed; all other adapters are blocked.

If the endpoint is in a location that defines only a Wi-Fi access point's SSID as the network identification(see "Wi-Fi Management" on page 104) , the Endpoint Security Client switches to that location before disabling the unauthorized adapter. A password override should be used to provide a manual location switch if this occurs.

The Endpoint Security Client receives notification whenever a network device is installed in the system and determines if the device is approved. If it is not approved, the solution disables the device driver, which renders this new device unusable, and notifies the user of the situation.

When a new unapproved adapter first installs its drivers on the endpoint (via PCMCIA or USB), the adapter displays as enabled in Windows Device Manager until the system is rebooted, though all network connectivity is blocked.

Storage Device Control

Storage device controls set the default storage device settings for the policy, where all external file storage devices are either allowed to read/write files, function in a read-only state, or be fully disabled. When disabled, these devices are rendered unable to retrieve any data from the endpoint; while the hard drive and all network drives remain accessible and operational.

NOTE: You can set the storage device controls globally on the *Global Policy Settings* tab or for individual locations on the *Locations* tab.

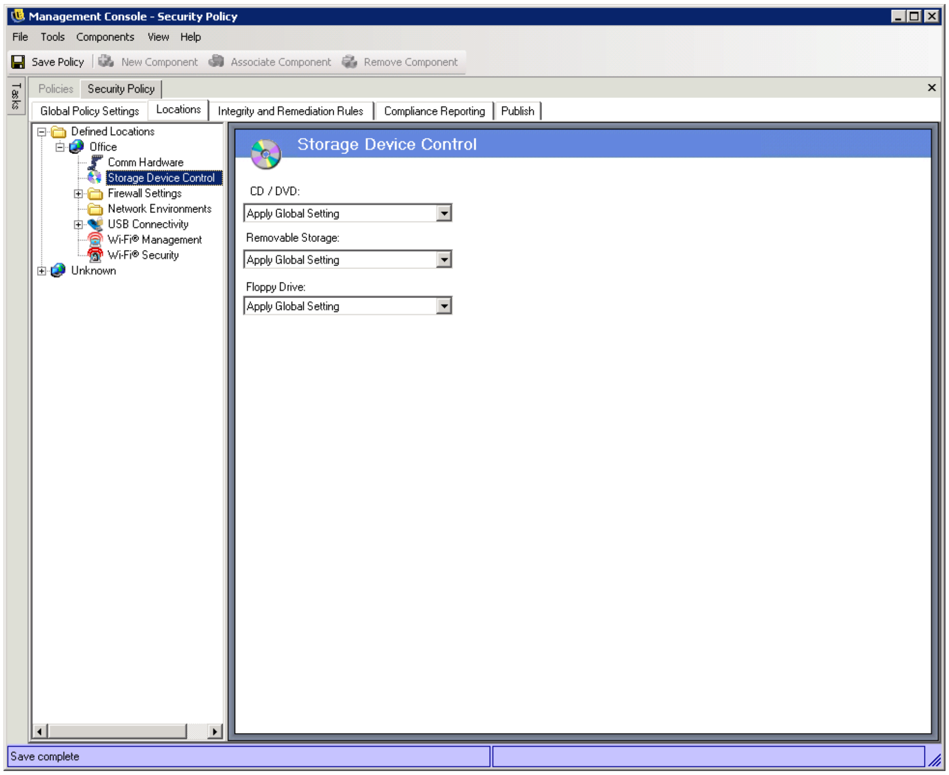
To access this control:

To set the storage device controls for a location, click the *Locations* tab, expand the desired location in the tree, then click *Storage Device Control*.

or

To set the storage device controls on a global basis, click the *Global Policy Settings* tab, expand *Global Settings* in the tree, then click *Storage Device Control*. For more information, see "Storage Device Control" on page 85.

Figure 6-19 Location Storage Device Control



Storage Device Control

CD / DVD: Apply Global Setting

Removable Storage: Apply Global Setting

Floppy Drive: Apply Global Setting

Save complete

Storage Device Control is differentiated into the following categories:

- **CD/DVD:** Controls all devices listed under *DVD/CD-ROM drives* in Windows Device Manager.
- **Removable Storage:** Controls all devices reporting as Removable storage under Disk drives in Windows Device Manager.
- **Floppy Drive:** Controls all devices listed under *Floppy disk drives* in Windows Device Manager.

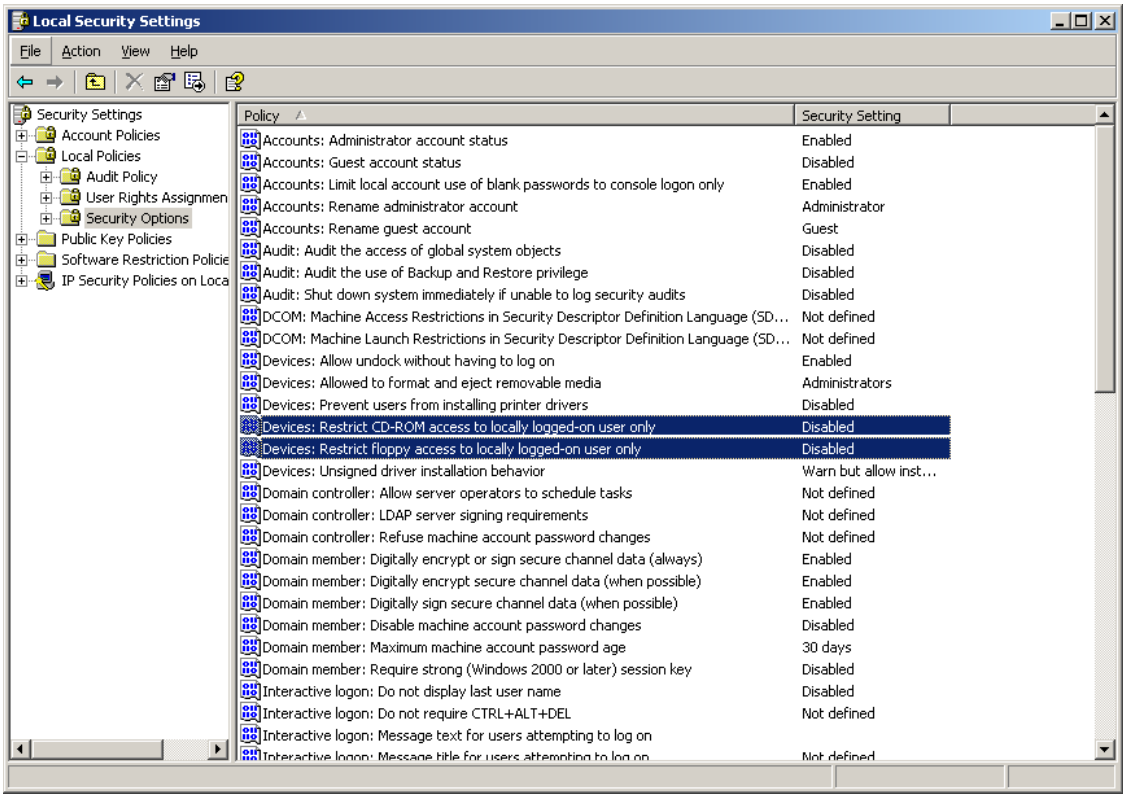
Fixed storage (hard disk drives) and network drives (when available) are always allowed.

To set the policy default for storage devices, select the global setting for both types from the drop-down lists:

- **Apply Global Setting:** Use the setting configured in the global Storage Device Control policy.
- **Allow All Access:** The device type is allowed by default.
- **Disable All Access:** The device type is disallowed. When users attempt to access files on a defined storage device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed
- **Read-Only Access:** The device type is set as Read-Only. When users attempt to write to the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed

NOTE: If you want to disable CD-ROM drives or floppy drives on a group of endpoints or set them as Read-Only, the Local Security Settings (passed down through a directory service group policy object) must have both Devices: Restrict CD-ROM access to locally logged-on user only and Devices: Restrict floppy access to locally logged-on user only set as Disabled. To verify this, open either the group policy object, or open Administrative Tools on a machine. Look in Local Security Settings - Security Options and verify both devices are disabled (see Figure 6-10). Disabled is the default.

Figure 6-20 *Verify Local Storage Device Options are set as Disabled*



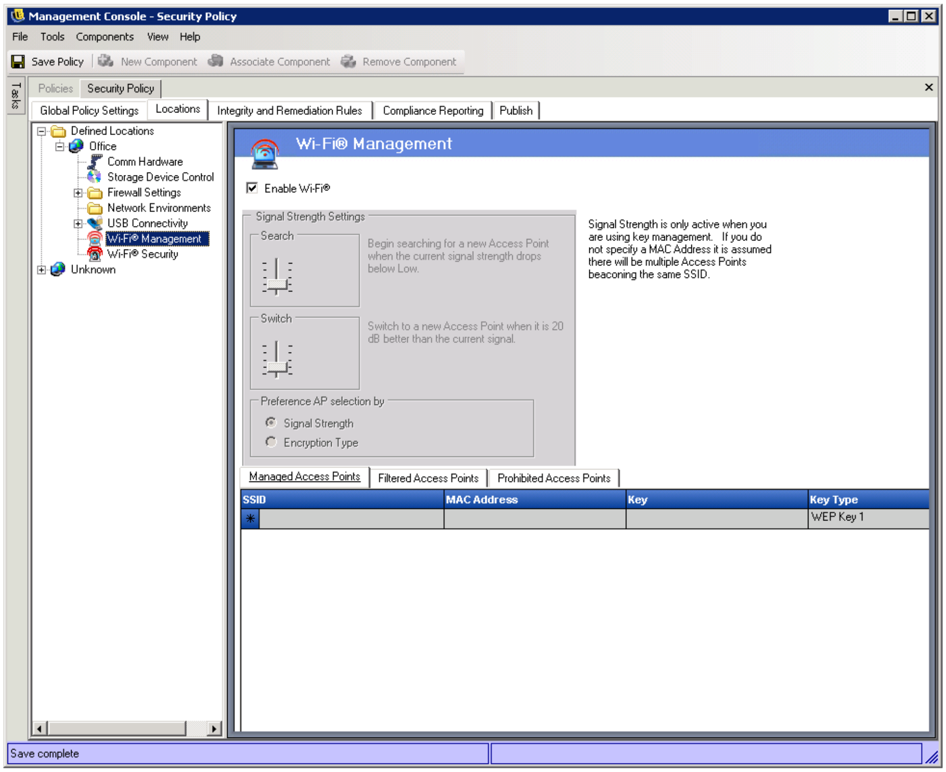
Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SD...	Not defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SD...	Not defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Devices: Unsigned driver installation behavior	Warn but allow inst...
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Not defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	Not defined

Wi-Fi Management

Wi-Fi management allows the administrator to create Access Point lists. The wireless access points entered into these lists determine which access points the endpoint is permitted and not permitted to connect to within the location, and which access points it's permitted to see in the Microsoft Zero Configuration Manager (Zero Config). Third-party wireless configuration managers are not supported with this functionality. If no access points are entered, all access points are available to the endpoint.

To access this control, click the *Locations* tab, then click *Wi-Fi Management* in the policy tree on the left.

Figure 6-21 *Location Wi-Fi Management*



Wi-Fi® Management

☑ Enable Wi-Fi®

Signal Strength Settings

Search: Begin searching for a new Access Point when the current signal strength drops below Low.

Switch: Switch to a new Access Point when it is 20 dB better than the current signal.

Preference AP selection by

● Signal Strength

○ Encryption Type

Signal Strength is only active when you are using key management. If you do not specify a MAC Address it is assumed there will be multiple Access Points beaconing the same SSID.

	SSID	MAC Address	Key	Key Type
*				WEP Key 1

Save complete

Entering access points into the Managed Access Points list turns off Zero Config and forces the endpoint to connect only to the access points listed when they're available. If the Managed access points are not available, the Endpoint Security Client falls back to the Filtered Access Point List. Access points entered into Prohibited Access Points never display in Zero Config.

NOTE: The access point list is only supported on the Windows XP operating system. Prior to deploying an access point list, it is recommended all endpoints clear the preferred networks list out of Zero Config.

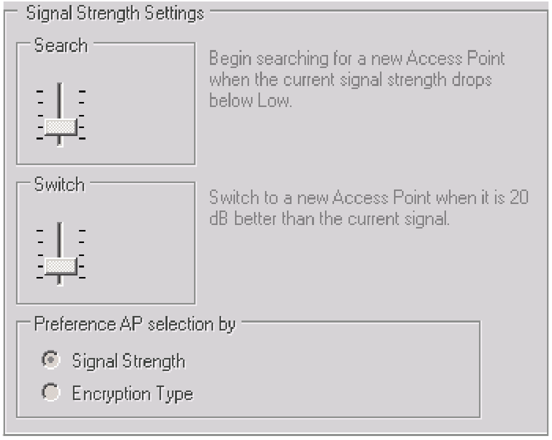
The following sections contain more information:

- "Wi-Fi Signal Strength Settings" on page 105
- "Managed Access Points" on page 107
- "Filtered Access Points" on page 108
- "Prohibited Access Points" on page 108

Wi-Fi Signal Strength Settings

When more than one WEP-managed access point is defined in the Managed Access Points list (see "Managed Access Points" on page 107), the signal strength switching for the Wi-Fi adapter can be set. The signal strength thresholds can be adjusted by location to determine when the Endpoint Security Client searches for, discards, and switches to another access point defined in the list.

Figure 6-22 Signal Strength Control



Signal Strength Settings

Search

Begin searching for a new Access Point when the current signal strength drops below Low.

Switch

Switch to a new Access Point when it is 20 dB better than the current signal.

Preference AP selection by

● Signal Strength

○ Encryption Type

The following settings can be adjusted above or below the current defaults:

- **Search:** When this signal strength level is reached, the Endpoint Security Client begins to search for a new access point to connect to. The default setting is Low [-70 dB].
- **Switch:** In order for the Endpoint Security Client to connect to a new access point, that access point must broadcast at the designated signal strength level above the current connection. The default setting is +20 dB.

The signal strength thresholds are determined by the amount of power (in dB) reported through the computer's miniport driver. As each Wi-Fi card and radio may treat the dB signals differently for their Received Signal Strength Indication (RSSI) the numbers vary from adapter to adapter.

The default numbers associated with the defined thresholds in the Management Console are generic for most Wi-Fi adapters. It is recommended you research your Wi-Fi adapter's RSSI values to input an accurate level. The Novell values are:

Name	Default Value
Excellent	-40 dB
Very Good	-50 dB
Good	-60 dB
Low	-70 dB
Very Low	-80 dB

Although the above signal strength names match those used by the Microsoft Zero Configuration Service, the thresholds may not match. Zero Config determines its values based on the Signal to Noise Ratio (SNR) and not solely on the dB value reported from RSSI. For example, if a Wi-Fi adapter were receiving a signal at -54 dB and had a noise level of -22 dB, the SNR would report as 32dB (-54 - -22=32), which on the Zero Configuration scale would translate as Excellent signal strength, even though on the Novell scale, the -54 dB signal (if reported that way through the miniport driver, possibly reported lower) would indicate a Very Good signal strength.

It's important to note that the end user never sees the Novell signal strength thresholds; this information is merely provided to show the difference between what the user may see through Zero Config and what is actually occurring behind the scenes.

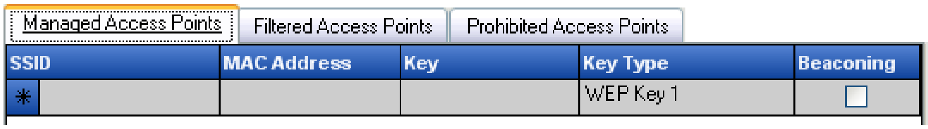
Because both signal strength and encryption type (see “Wi-Fi Security” on page 108) are used to determine the order in which access points are attempted, you must select the preferred method. For example, if signal strength is the preference, then the strongest signal is given the preference when connecting. If WEP 64 is the encryption requirement and encryption is the preference, then access points with the highest encryption strength are given preference over all others.

Managed Access Points

ZENworks Endpoint Security Management provides a simple process to automatically distribute and apply Wired Equivalent Privacy (WEP) keys without user intervention (bypassing and shutting down the Microsoft Zero Configuration manager), and protects the integrity of the keys by not passing them in the clear over an e-mail or a written memo. In fact, the end user never needs to know the key to automatically connect to the access point. This helps prevent possible re-distribution of the keys to unauthorized users.

Due to the inherent security vulnerabilities of Shared WEP Key Authentication, Novell supports only Open WEP Key Authentication. With Shared Authentication the client/AP key validation process sends both a clear text and encrypted version of a challenge phrase that is easily sniffed wirelessly. This can give a hacker both the clear and encrypted versions of a phrase. Once they have this information, cracking the key becomes trivial.

Figure 6-23 *Managed Access Points Control*



SSID	MAC Address	Key	Key Type	Beaconing
*			WEP Key 1	□

Enter the following information for each access point:

- **SSID:** Identify the SSID number. The SSID number is case sensitive.
- **MAC Address:** Identify the MAC Address (recommended, due to the commonality among SSIDs. If not specified, it is assumed there are multiple access points beaconing the same SSID number).
- **Key:** Specify the WEP key for the access point (either 10 or 26 hexadecimal characters).
- **Key Type:** Identify the encryption key index by selecting the appropriate level from the drop-down list.
- **Beaconing:** Check if the defined access point is currently broadcasting its SSID. Leave un-checked if this is a non-beaconing access point.

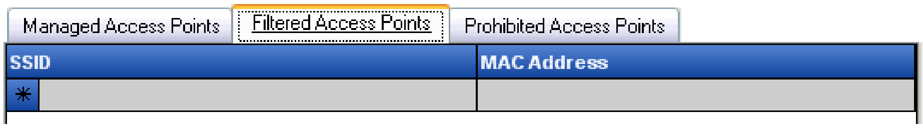
The Endpoint Security Client attempts to first connect to each beaconing access point listed in the policy. If no beaconing access is located, the Endpoint Security Client then attempts to connect to any non-beaconing access points (identified by SSID) listed in the policy.

When one or more access points are defined in the *Managed Access Points* list, the Signal Strength switching for the Wi-Fi adapter can be set (see “Wi-Fi Signal Strength Settings” on page 105).

Filtered Access Points

Access points entered into the *Filtered Access Points* list are the only access points that display in Zero Config; this prevents an endpoint from connecting to unauthorized access points.

***Figure 6-24** Filtered Access Points Control*



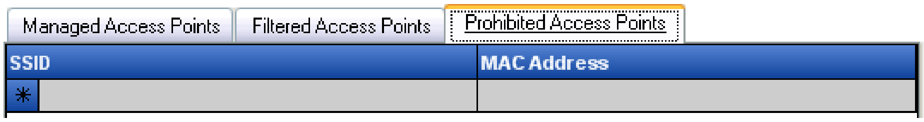
Enter the following information for each access point:

- **SSID:** Identify the SSID number. The SSID number is case sensitive.
- **MAC Address:** Identify the MAC Address (recommended, due to the commonality among SSIDs. If not specified, it is assumed there will be multiple access points beaconing the same SSID).

Prohibited Access Points

Access points entered into the *Prohibited Access Points* list do not display in Zero Config, nor will the endpoint be permitted to connect to them.

***Figure 6-25** Prohibited Access Points Control*



Enter the following information for each access point:

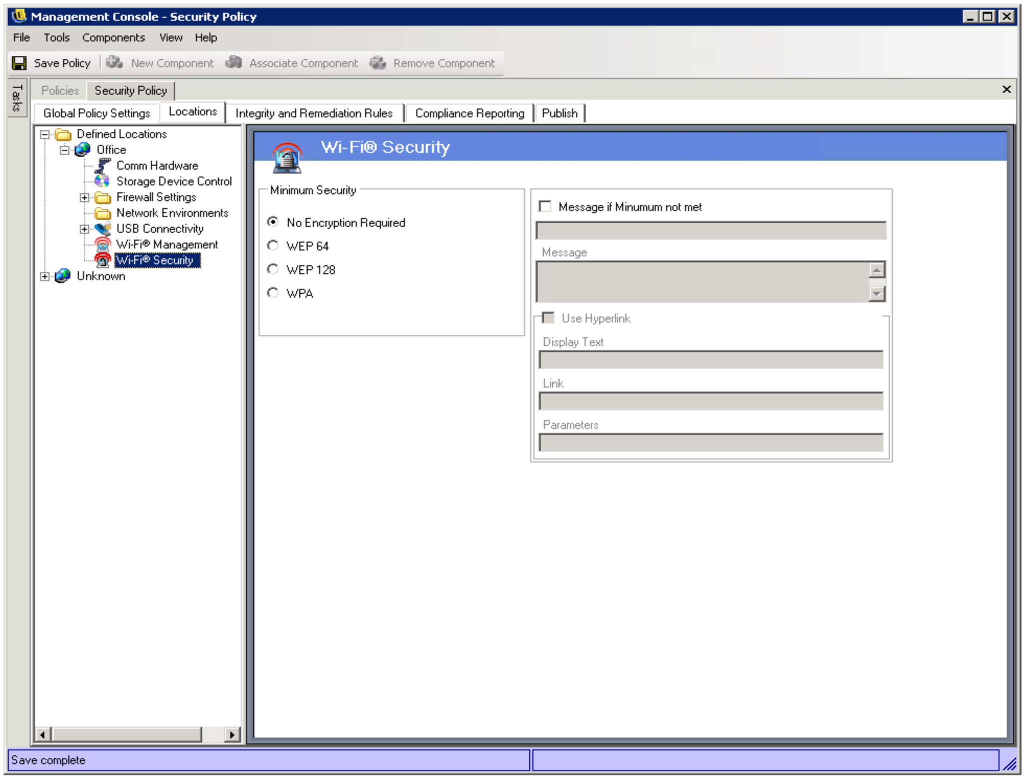
- **SSID:** Identify the SSID number. The SSID number is case sensitive.
- **MAC Address:** Identify the MAC Address (recommended, due to the commonality among SSIDs. If not specified, it is assumed there will be multiple access points beaconing the same SSID).

Wi-Fi Security

If Wi-Fi Communication Hardware (Wi-Fi adapter PCMCIA or other cards, and built-in Wi-Fi radios) is globally permitted (see "Wireless Control" on page 82), additional settings can be applied to the adapter at this location.

To access this control, click the *Locations* tab, then click *Wi-Fi Security* in the policy tree on the left.

Figure 6-26 Location Wi-Fi Security



Wi-Fi® Security

Minimum Security

● No Encryption Required
○ WEP 64
○ WEP 128
○ WPA

□ Message if Minumum not met

Message

□ Use Hyperlink

Display Text

Link

Parameters

The Wi-Fi adapter can be set to communicate only with access points with a specific level of encryption or greater in a given location.

For example, if a WPA configuration of access points were deployed in a branch office, the adapter can be restricted to only communicate with access points with a level of WEP 128 encryption or greater, thus preventing it from accidentally associating with rogue, non-secure access points.

It is recommended a custom user message be written when the setting is placed above *No Encryption Required*.

A preference can be set to connect to access points by order of encryption level or by signal strength when two or more access points are entered into the *Managed* and *Filtered Access Points* lists. The level selected enforces connectivity with access points that meet the minimum encryption requirement or greater.

For example, if WEP 64 is the encryption requirement and encryption is the preference, then access points with the highest encryption strength are given preference over all others. If signal strength is the preference, then the strongest signal is given the preference when connecting.

6.2.3 Integrity and Remediation Rules

ZENworks Endpoint Security Management provides the ability to verify that required software is running on the endpoint and provides instant remediation procedures if the verification fails.

The following sections contain more information:

- “Antivirus/Spyware Rules” on page 110

- "Integrity Tests" on page 112
- "Integrity Checks" on page 113
- "Advanced Scripting Rules" on page 114

Antivirus/Spyware Rules

Antivirus/Spyware Rules verify that designated antivirus or spyware software on the endpoint is running and up to date. Tests are run to determine if the software is running and if the version is up-to-date. Success in both checks allow switching to any defined locations. Failure of either test could result in any or all of the following actions (defined by the administrator):

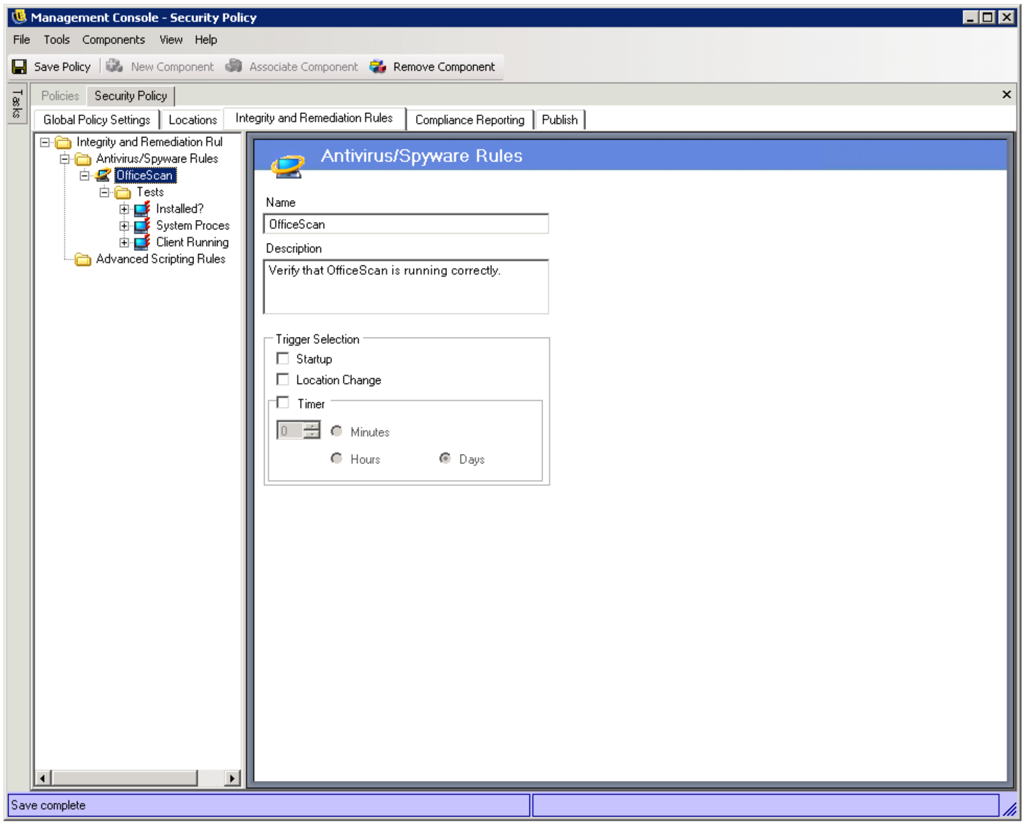
- A report is sent to the Reporting Service.
- A custom user message is displayed, with an optional launch link that provides information on how to fix the rule violation.
- The user is switched to a Quarantined State, which limits the user's network access and disallows certain programs from accessing the network to prevent the user from further infecting the network.

After endpoints are determined compliant by a follow-up test, security settings automatically return to their original state.

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for UWS security policies.

To access this control, click the *Integrity and Remediation Rules* tab, then click *Antivirus/Spyware Rules* in the policy tree on the left.

Figure 6-27 *Antivirus/Spyware Integrity rules*



Name: OfficeScan

Description: Verify that OfficeScan is running correctly.

Trigger Selection

□ Startup

□ Location Change

□ Timer

0 ○ Minutes ○ Hours ● Days

Save complete

Custom tests for software not on the default list can be created. A single test can be created to run checks for one or more software pieces within the same rule. Each set of Process Running and File Exists checks have their own success/failure results.

To create a new antivirus/spyware rule:

1. Select *Antivirus/Spyware Rules* from the components tree, then click *New Antivirus/Spyware*.
2. Click *New Component*.
3. Name the rule and provide a description.
4. Select the trigger for the rule:
   - **Startup:** Run tests at system startup.
   - **Location Change:** Run the tests whenever the Endpoint Security Client switches to a new location.
   - **Timer:** Run integrity tests on a defined schedule by the minute, hour, or day.
5. Click *Save Policy*.
6. Define the integrity tests.

To associate existing Antivirus/Spyware Rules:

1. Select *Antivirus/Spyware Rules*, then click *Associate Component*.
2. Select the desired rules from the list.
3. If desired, you can redefine the tests, checks, and results.

NOTE: Changing the settings in a shared component affects all other instances of this same component. Use the *Show Usage* command to view all other policies associated with this component.

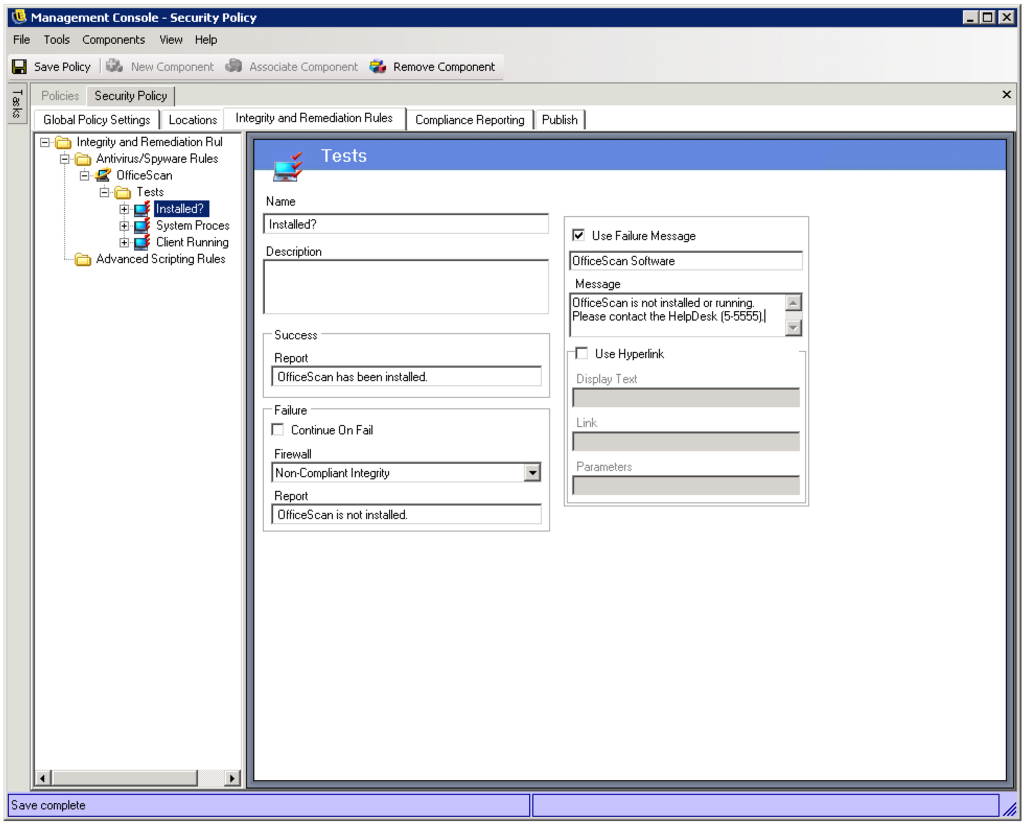
4 Click *Save Policy*.

Integrity tests and checks are automatically included and can be edited as necessary.

Integrity Tests

Each integrity test can run two checks, *File Exists* and *Process Running*. Each test has its own success and fail results.

Figure 6-28 *Integrity Tests*



Name: Installed?

Description:

Success

Report: OfficeScan has been installed.

Failure

☐ Continue On Fail

Firewall: Non-Compliant Integrity

Report: OfficeScan is not installed.

☑ Use Failure Message

OfficeScan Software

Message: OfficeScan is not installed or running. Please contact the HelpDesk (5-5555).

☐ Use Hyperlink

All defined antivirus/spyware rules have standard tests and checks pre-written. Additional tests can be added to the integrity rule.

Multiple tests run in the order entered here. The first test must complete successfully before the next test runs.

To create an integrity test:

1 Select *Integrity Tests* on the component tree, click the plus sign icon next to the desired report to expand the list, right-click *Tests*, then click *Add New Tests*.

2 Name the test and provide a description.

3 Enter the success report text for the test.

4 Define the following for a test failure:

- **Continue on Fail:** Check this if the user can continue to network connectivity if the test fails, or if the test should repeat.
- **Firewall:** This setting is applied if the test fails. All Closed, Non-compliant Integrity, or a custom Quarantine firewall setting prevents the user from connecting to the network.
- **Message:** Select a custom user message to be displayed at test failure. This can include remediation steps for the end user.
- **Report:** Enter the failure report that is sent to the reporting service.

5 Enter a Failure Message. This message displays only when one or more of the checks fail. Click the check box, then enter the message information in the provided boxes.

6 A hyperlink can be added to provide remediation options. This can be a link to more information or a link to download a patch or update for the test failure (see Section 6.3.4, “Hyperlinks,” on page 124.)

7 Click *Save Policy*.

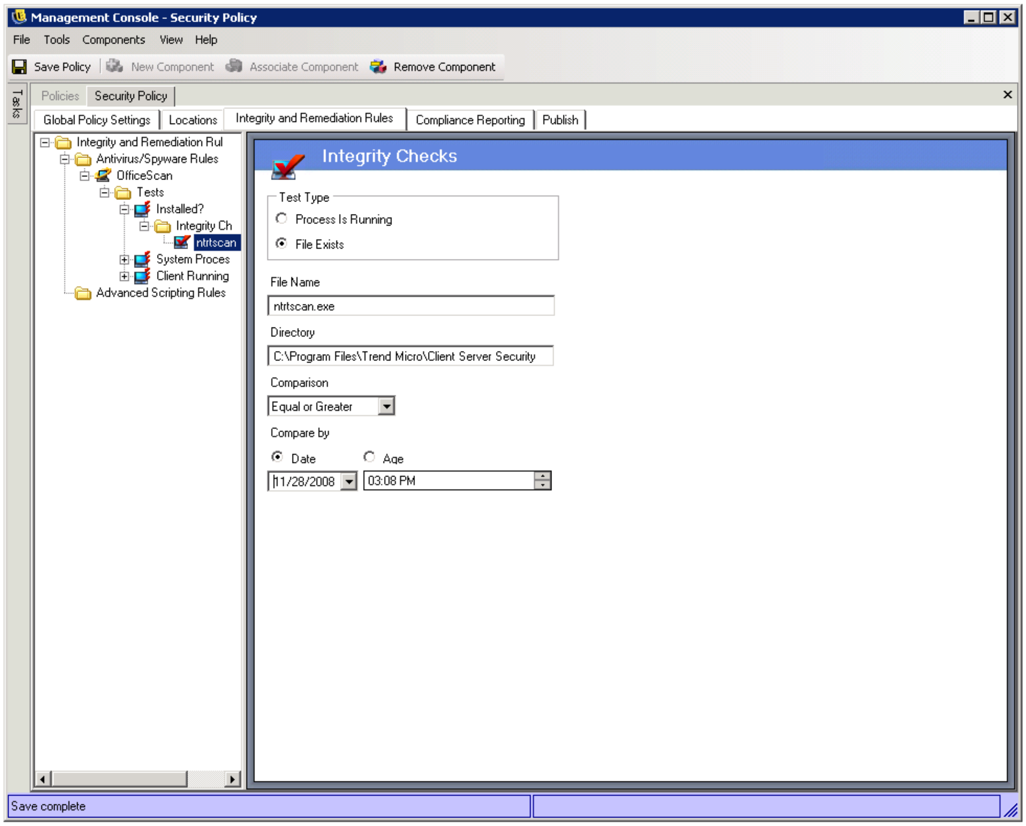
8 Define the integrity checks.

9 Repeat the above steps to create a new antivirus/spyware test

Integrity Checks

The checks for each test determine if one or more of the antivirus/spyware process is running or if essential files exist. At least one check must be defined for an integrity test to run.

Figure 6-29 *Integrity Checks*



Test Type
○ Process Is Running
● File Exists

File Name: ntrtscan.exe

Directory: C:\Program Files\Trend Micro\Client Server Security

Comparison: Equal or Greater

Compare by
● Date ○ Age

11/28/2008 03:08 PM

Save complete

To create a new check, right-click Integrity Checks from the policy tree on the left, then click *Add New Integrity Checks*. Select one of the two check types and enter the information described below:

Process is Running

This check is used to determine if the software is running at the time of the triggering event (i.e., the AV client). The only information required for this check is the executable name.

File Exists

This check is used to determine if the software is current and up-to-date at the time of the triggering event.

Enter the following information in the provided fields:

- **File Name:** Specify the filename that you want to check.
- **File Directory:** Specify the directory where the file resides.
- **File Comparison:** Select a date comparison from the drop-down list:
  - None
  - Equal
  - Equal or Greater
  - Equal or Less
- **Compare by:** Specify *Age* or *Date*.
  - *Date* ensures that the file is no older than a specified date and time (for example, the date of the last update).
  - *Age* ensures that the file is no older than a specific time period, measured in days.

NOTE: The Equal file comparison is treated as Equal or Less when using the *Age* check.

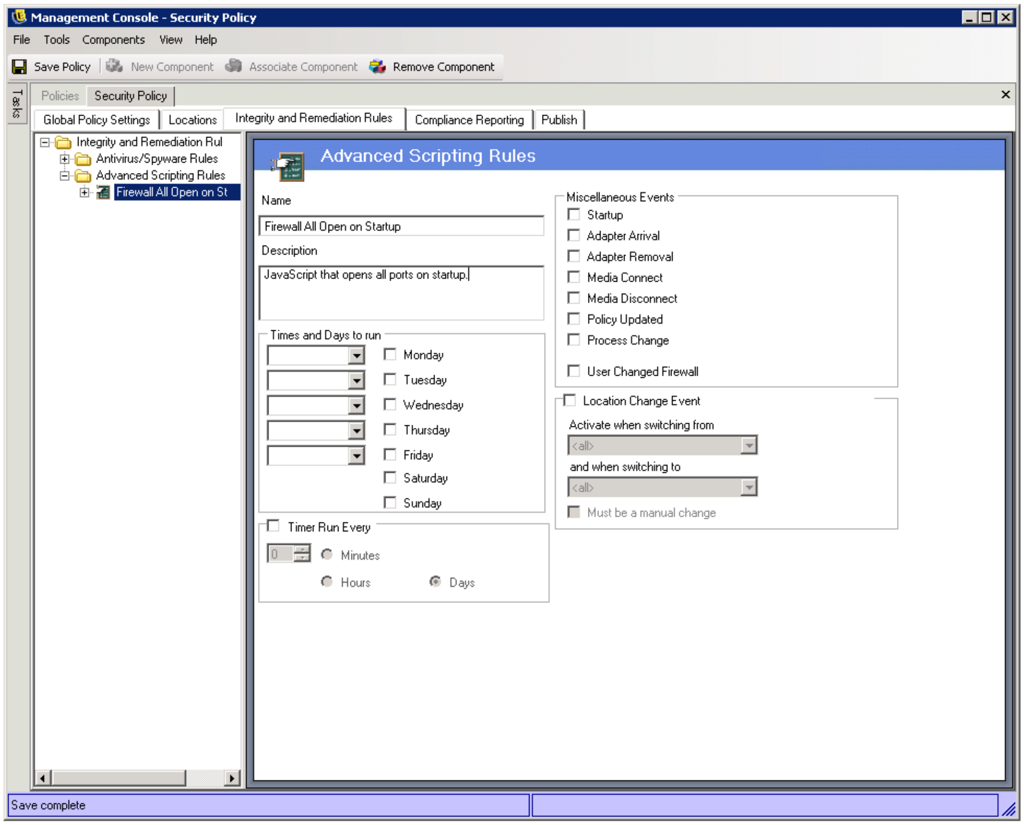
The checks are run in the order entered.

Advanced Scripting Rules

ZENworks Endpoint Security Management includes an advanced rule scripting tool that gives administrators the ability to create extremely flexible and complex rules and remediation actions.

To access this control, click the *Integrity and Remediation Rules* tab, then click the *Advanced Scripting Rules* icon in the policy tree on the left.

Figure 6-30 *Advanced Scripting*



Name Firewall All Open on Startup

Description JavaScript that opens all ports on startup.

Times and Days to run

□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

□ Timer Run Every 0 ○ Minutes ○ Hours ● Days

Miscellaneous Events

□ Startup
□ Adapter Arrival
□ Adapter Removal
□ Media Connect
□ Media Disconnect
□ Policy Updated
□ Process Change
□ User Changed Firewall

□ Location Change Event

Activate when switching from <all>

and when switching to <all>

□ Must be a manual change

The scripting tool uses either of the common scripting languages, VBScript or JScript, to create rules that contain both a trigger (when to execute the rule) and the actual script (the logic of the rule). The administrator is not restricted on the type of script to be run.

Advanced scripting is implemented sequentially, along with other integrity rules. Therefore, a long-running script will prevent other rules (including timed rules) from executing until that script is complete.

To create a new advanced scripting rule:

1. Right-Click *Advanced Scripting Rules* from the components tree, then click *Add New Scripting Rules*.
2. Name the rule and provide a description.
3. Specify the triggering event(s)
   - **Times and Days to Run:** Specify as many as five different times for the script to run. The script runs weekly, on the selected day(s).
   - **Timer Run Every:** Specify how often to run the timer.
   - **Miscellaneous Events:** Specify the events on the endpoint that trigger the script.
   - **Location Change Event:** Specify the location change event that triggers the script. These events are not independent; they are additive to the previous event.
     - **Check Location Event:** The script runs at all location changes.

- **Activate when switching from:** The script runs only when the user leaves this (specified) location to any other location.
- **Activate when switching to:** The script runs when the user enters this (specified) location from any other location (if *Activate when switching from* was given a location parameter (example: office), the script runs only when the location switches from office to the specified location).
- **Must be a manual change:** The script runs only when the user manually switches from or to a location.

4 Create any Script Variables. For more information see "Script Variables" on page 116.

5 Write the Script Text. For more information, see "Script Text" on page 117.

6 Click *Save Policy*.

To associate an existing advanced scripting rule:

1 Select Advanced Scripting Rules in the components tree and click Associate New

2 Select the desired rule(s) from the list

3 The trigger event, variables, or script may be re-defined

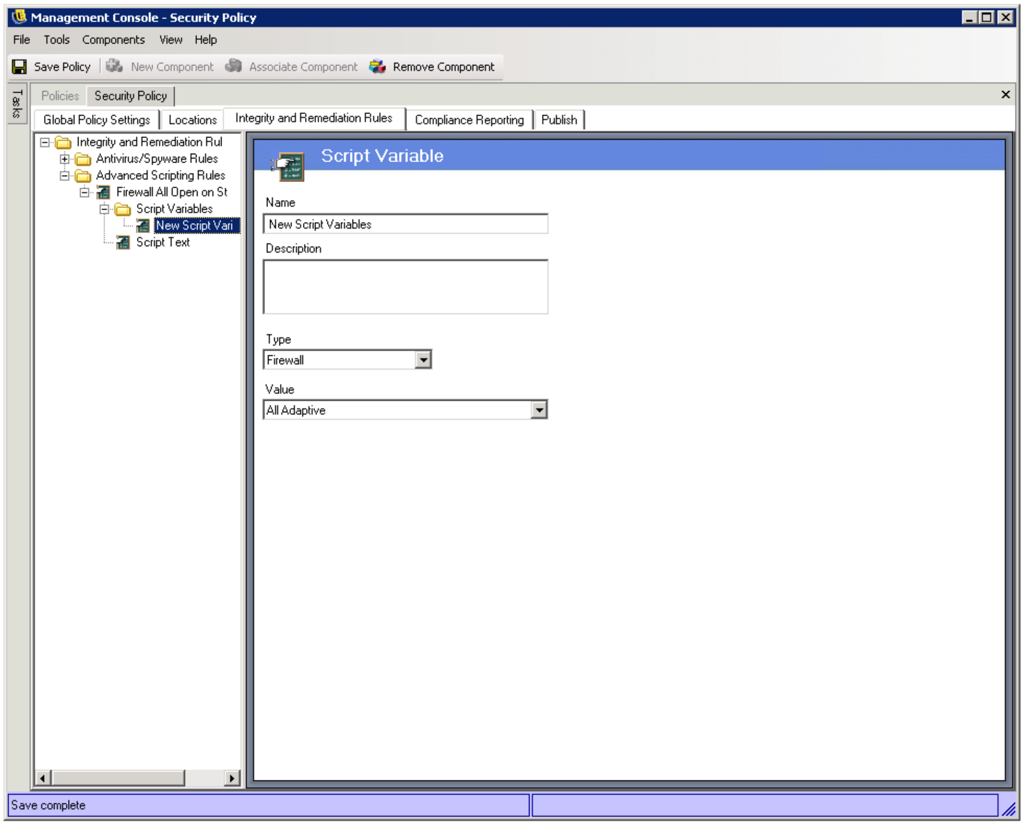
> **NOTE:** Changing the settings in a shared component will affect ALL OTHER instances of this same component. Use the Show Usage command to view all other policies associated with this component.

4 Click Save

Script Variables

This is an optional setting, which permits the Administrator to define a variable (var) for the script and either be able to use ZENworks Endpoint Security Management functionality (i.e., launch defined custom user messages or hyperlink; switch to a defined location or firewall setting) or have the freedom to change the value of a variable without changing the script itself.

Figure 6-31 *Script Variables*



Name: New Script Variables

Description:

Type: Firewall

Value: All Adaptive

Save complete

To create a new script variable:

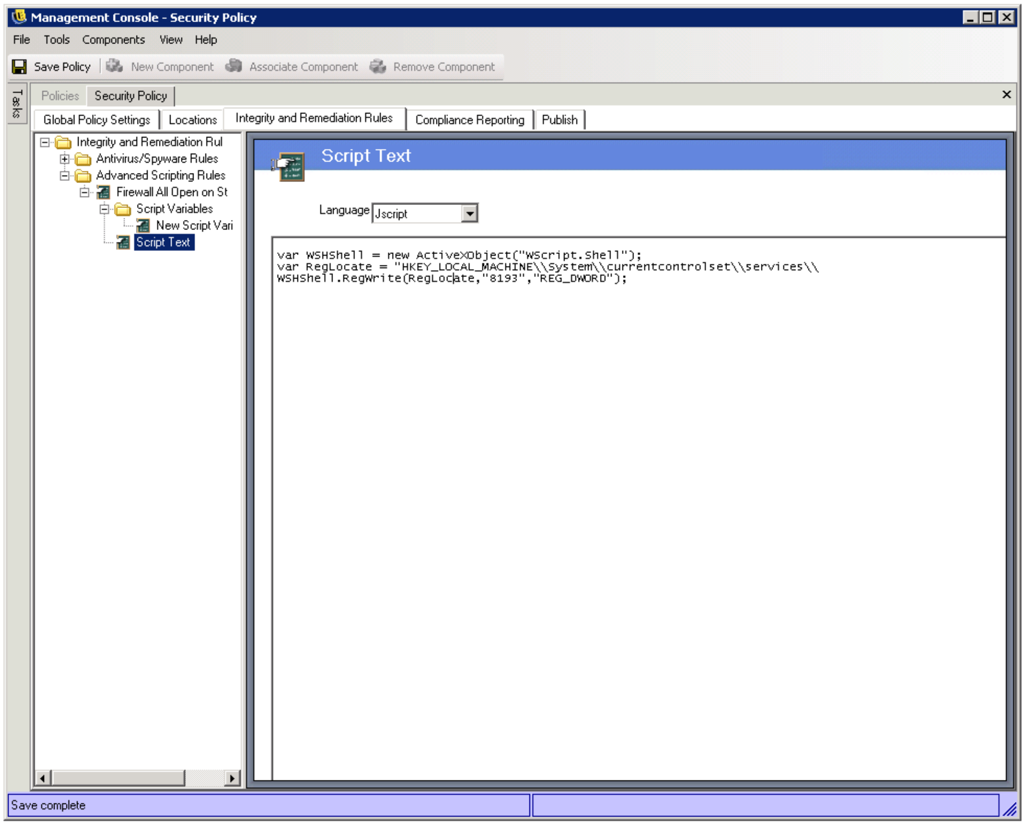
1. Select Script Variables from the components tree and click Add New
2. Name the variable and provide a description
3. Select type of variable:
   - **Custom User Messages -** defines a custom user message which can launch as an action
   - **Firewall -** defines a firewall setting which can be applied as an action
   - **Hyperlinks -** defines a hyperlink which can be launched as an action
   - **Location -** defines a location which can be applied as an action
   - **Number -** defines a number value
   - **String -** defines a string value
4. Select/enter the value of the variable
5. Click Save. Repeat the above steps to create a new variable

Script Text

The ZENworks Endpoint Security Management Administrator is not limited to the type of script the Endpoint Security Client may execute. It is recommended that ANY script be tested prior to distributing the policy.

Select the script type (Jscript or VBscript) and enter the script text in the provided field. The script may be copied from another source and pasted into the field. See Section 6.3.11, “Rule Scripting Parameters,” on page 138, for acceptable script syntax.

Figure 6-32 *Script Text Window*



Management Console - Security Policy
File Tools Components View Help
Save Policy New Component Associate Component Remove Component
Tasks
Policies Security Policy
Global Policy Settings Locations Integrity and Remediation Rules Compliance Reporting Publish
Integrity and Remediation Rul
Antivirus/Spyware Rules
Advanced Scripting Rules
Firewall All Open on St
Script Variables
New Script Vari
Script Text
Script Text
Save complete

Language Jscript

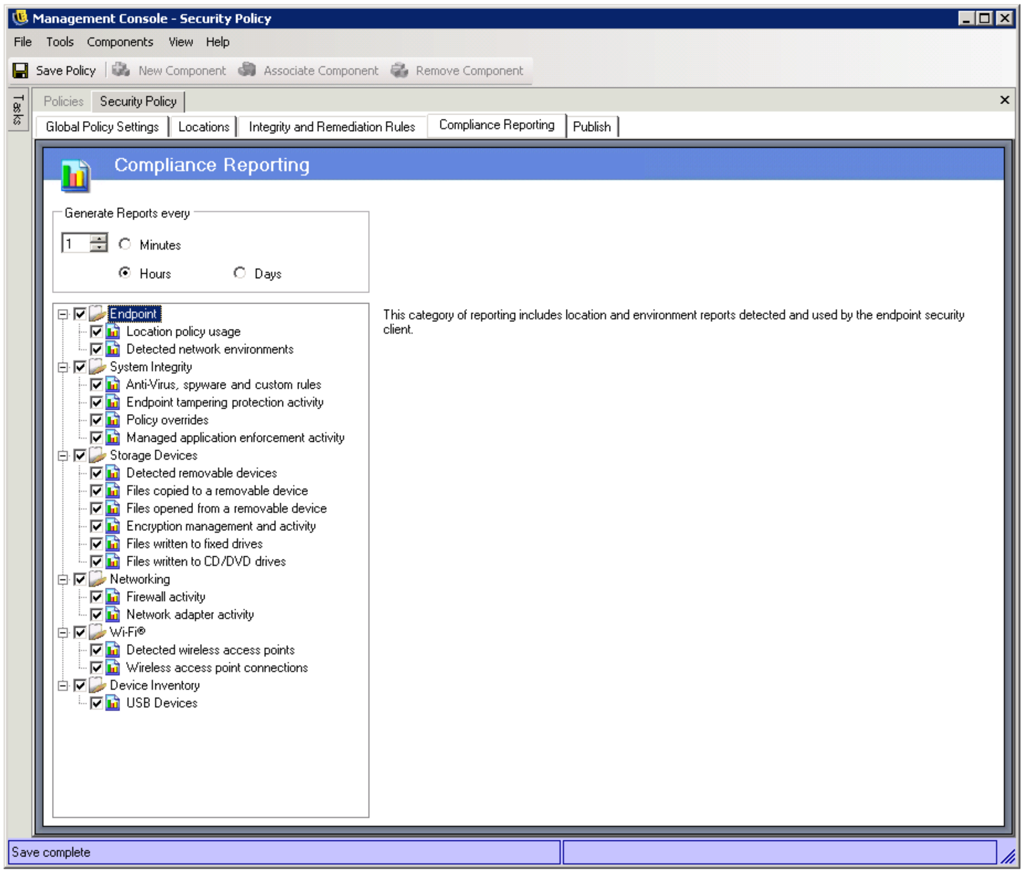
```
var WSHShell = new ActiveXObject("WScript.Shell");
var RegLocate = "HKEY_LOCAL_MACHINE\\System\\currentcontrolset\\services\\
WSHShell.RegWrite(RegLocate,"8193","REG_DWORD");
```

6.2.4 Compliance Reporting

Because of the level and access of the Endpoint Security Client's drivers, virtually every transaction the endpoint performs can be reported. The endpoint can have each optional system inventory run for troubleshooting and policy creation purposes. To access this control, open the Compliance Reporting tab.

NOTE: Reporting is not available when running the Stand-Alone Management Console

Figure 6-33 Compliance Reporting



Generate Reports every

1 ○ Minutes

● Hours ○ Days

- ☑ Endpoint
  - ☑ Location policy usage
  - ☑ Detected network environments
- ☑ System Integrity
  - ☑ Anti-Virus, spyware and custom rules
  - ☑ Endpoint tampering protection activity
  - ☑ Policy overrides
  - ☑ Managed application enforcement activity
- ☑ Storage Devices
  - ☑ Detected removable devices
  - ☑ Files copied to a removable device
  - ☑ Files opened from a removable device
  - ☑ Encryption management and activity
  - ☑ Files written to fixed drives
  - ☑ Files written to CD/DVD drives
- ☑ Networking
  - ☑ Firewall activity
  - ☑ Network adapter activity
- ☑ Wi-Fi®
  - ☑ Detected wireless access points
  - ☑ Wireless access point connections
- ☑ Device Inventory
  - ☑ USB Devices

This category of reporting includes location and environment reports detected and used by the endpoint security client.

Save complete

To run compliance reporting for this policy, perform the following steps:

1. Define the Send Time. This is the timeframe that data will be uploaded from the Endpoint Security Client to the Policy Distribution Service.
2. Check each report category, or type, you wish to capture.

The following reporting features are available:

Endpoint

- **Location policy usage** - the Endpoint Security Client will report all location policies enforced and the duration of that enforcement
- **Detected network environments** - the Endpoint Security Client will report all detected network environment settings

System Integrity

- **Anti-virus, spyware, and custom rules** - the Endpoint Security Client will report the configured integrity messages based on test results
- **Endpoint tampering protection activity** - the Endpoint Security Client will report any attempts to tamper with the security client

- **Policy overrides -** the Endpoint Security Client will report all attempts to initiate the administrative override on the security client
- **Managed application enforcement activity -** the Endpoint Security Client will report all enforcement activities for managed applications

Storage Devices

- **Detected removable devices -** the Endpoint Security Client will report all removable storage devices detected by the security client
- **Files copied to a removable device -** the Endpoint Security Client will report files that are copied to a removable storage device
- **Files opened from a removable device -** the Endpoint Security Client will report files that are opened from a removable storage device
- **Encryption management and activity -** the Endpoint Security Client will report encryption/ decryption activity using SES
- **Files written to fixed drives -** the Endpoint Security Client will report the number of files that have been written to the machine's fixed drives
- **Files written to CD -** the Endpoint Security Client will report the number of files that have been written to the machine's CD and DVD drives

Networking

- **Firewall activity -** the Endpoint Security Client will report all traffic blocked by the firewall configured for the applied location policy. Enabling this report may result in large volumes of data being gathered

WARNING: The following data can overwhelm a database very quickly when gathered. A test of ONE Endpoint Security Client reported 1,115 data uploads of blocked packets over a 20 hour period. It is recommended that a monitoring and tuning period with a test client in the affected environment be run prior to wide-scale deployment.

- **Network adapter activity -** the Endpoint Security Client will report all traffic activity for a managed network device

Wi-Fi®

- **Detected wireless access points -** the Endpoint Security Client will report all detected access points
- **Wireless access point connections -** the Endpoint Security Client will report all access point connections made by the endpoint

Device Inventory

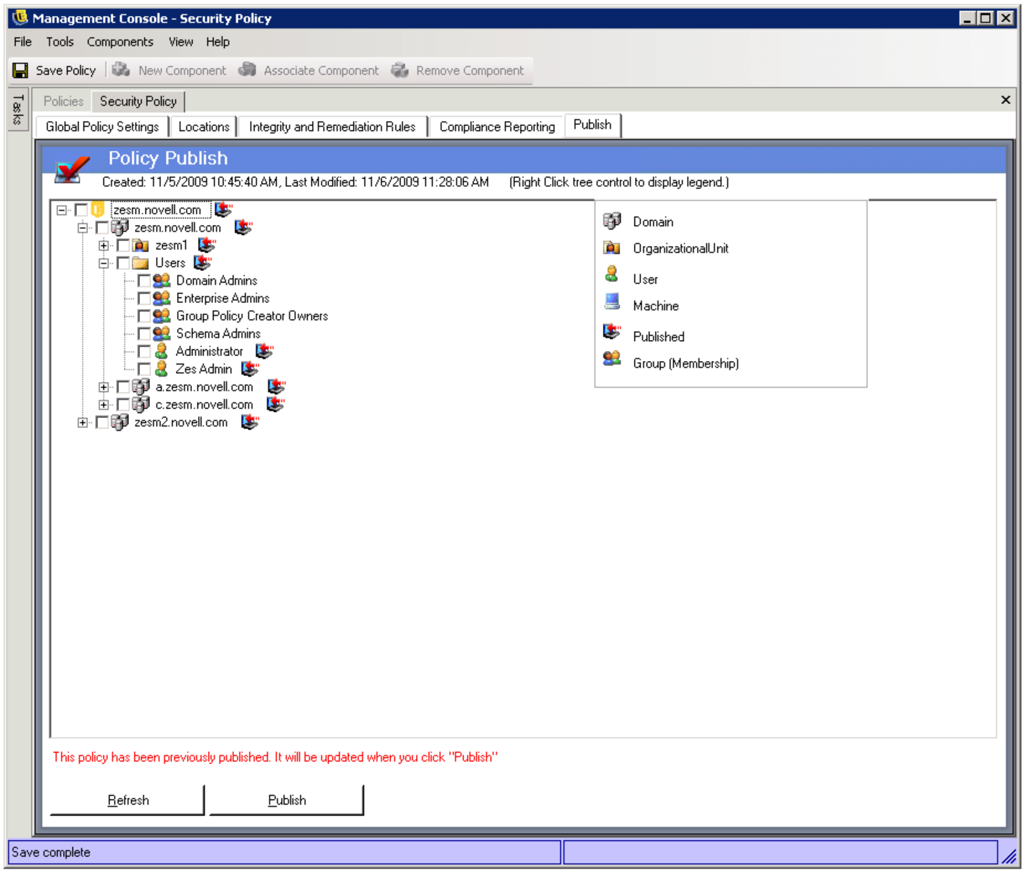
- **USB Devices -** the Endpoint Security Client will report all USB devices

6.2.5 Publishing Security Policies

Completed security policies are sent to the end-users using the publishing mechanism. Once a policy has been published, it can be further updated with the end-user receiving updates at their scheduled check-ins. To publish a policy, click the Publish tab. The following information is displayed:

- The current directory tree
- The policy's created and modified dates
- The Refresh and Publish buttons

Figure 6-34 *Publish a Security Policy*



Created: 11/5/2009 10:45:40 AM, Last Modified: 11/6/2009 11:28:06 AM (Right Click tree control to display legend.)

This policy has been previously published. It will be updated when you click "Publish"

Save complete

Based on the current user's publishing permissions, the directory tree may display with one or more of the selections in red. Users will NOT be permitted to publish to any users/groups displayed in red.

Users and their associated groups will not display until they have authenticated to the Management Service. Changes in the corporate directory service may not immediately display in the Management Console. Click Refresh to update the directory tree for the Management Service.

To publish a policy, perform the following steps:

1. Select a user or computer group (or single user or computer) from the directory tree.
2. Click Publish.

Updating a Published Policy

Once a policy has been published to the user(s) or computer(s), simple updates can be maintained by editing the components in a policy, and re-publishing. For example, if the ZENworks Endpoint Security Management Administrator needs to change the WEP key for an access point, the adminstrator only needs to edit the key, save the policy, and click Publish. The affected end-users and computers receive the updated policy (and the new key) at their next check-in.

6.3 Managing Policies

The following sections contain more information:

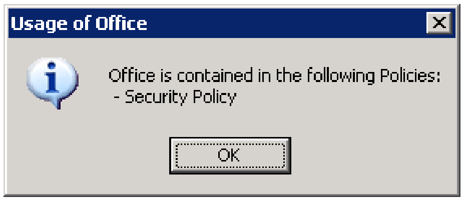
- Section 6.3.1, "Show Usage," on page 122
- Section 6.3.2, "Error Notification," on page 122
- Section 6.3.3, "Custom User Messages," on page 123
- Section 6.3.4, "Hyperlinks," on page 124
- Section 6.3.5, "Defined Location Settings," on page 125
- Section 6.3.6, "Network Environments," on page 126
- Section 6.3.7, "Firewall Settings," on page 128
- Section 6.3.8, "TCP/UDP Ports," on page 130
- Section 6.3.9, "Access Control Lists," on page 134
- Section 6.3.10, "Application Controls," on page 136
- Section 6.3.11, "Rule Scripting Parameters," on page 138

6.3.1 Show Usage

Changes made to shared policy components will affect all policies they are associated with. Prior to updating or otherwise changing a policy component, it is recommended that you run the Show Usage command to determine which policies will be affected by the change.

1. Right-click the component and select Show Usage
2. A pop-up window will display, showing each instance of this component in other policies (see Figure 6-35).

Figure 6-35 *Show Usage Window*



Usage of Office

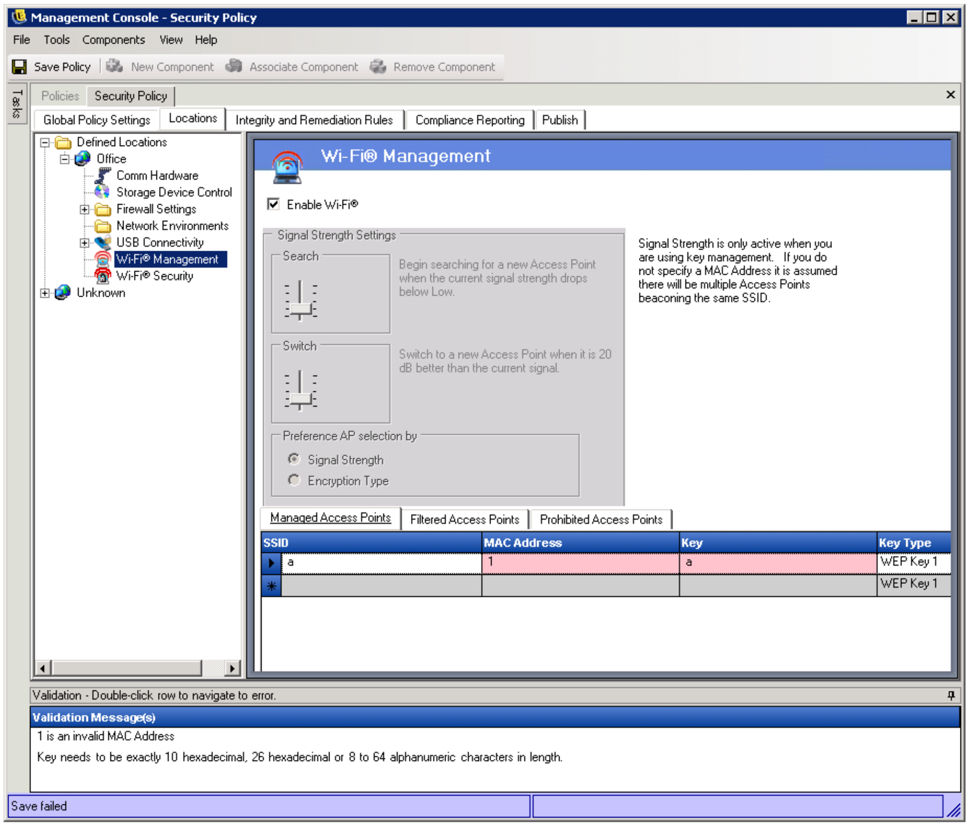
Office is contained in the following Policies:
- Security Policy

6.3.2 Error Notification

When the administrator attempts to save a policy with incomplete or incorrect data in a component, the Validation pane will display at the bottom of the Management console, highlighting each error. The errors MUST be corrected before the policy can be saved.

Double-click each validation row to navigate to the screen with the error. Errors are highlighted as shown in the figure below (see Figure 6-36).

***Figure 6-36** Error Notification Pane*



☑ Enable Wi-Fi®

Begin searching for a new Access Point when the current signal strength drops below Low.

Switch to a new Access Point when it is 20 dB better than the current signal.

● Signal Strength
○ Encryption Type

Signal Strength is only active when you are using key management. If you do not specify a MAC Address it is assumed there will be multiple Access Points beaconing the same SSID.

SSID	MAC Address	Key	Key Type
a	1	a	WEP Key 1
			WEP Key 1

Validation - Double-click row to navigate to error.

Validation Message(s)

1 is an invalid MAC Address

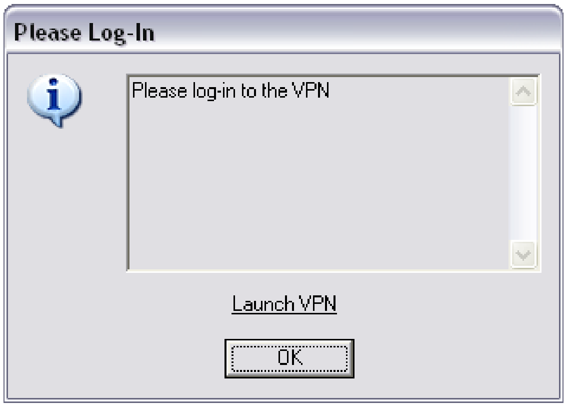
Key needs to be exactly 10 hexadecimal, 26 hexadecimal or 8 to 64 alphanumeric characters in length.

Save failed

6.3.3 Custom User Messages

Custom User Messages allow the ZENworks Endpoint Security Management Administrator to create messages which directly answer security policy questions as the user encounters policy enforced security restrictions, or provide specific instructions to the user. User messages controls (see Figure 6-37) are available in various components of the policy.

***Figure 6-37** Custom User Message with a Hyperlink*

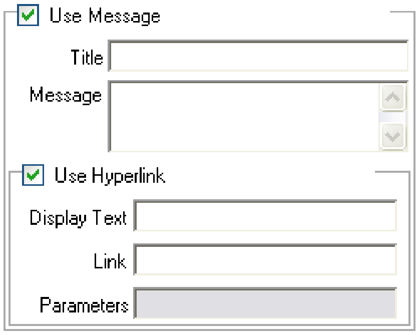


Please log-in to the VPN

To create a custom user message, perform the following steps (Figure 6-38 on page 124 for an example of the control):

1. Enter a title for the message. This displays on the top bar of the message box (see example in Figure 6-36 on page 123 above)
2. Enter the message. The message is limited to 1000 characters
3. If a hyperlink is required, check the hyperlinks box and enter the necessary

***Figure 6-38** Custom Message and Hyperlink Controls*

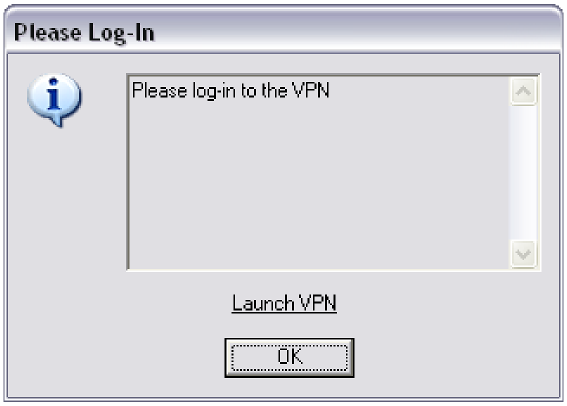


NOTE: Changing the Message or Hyperlink in a shared component will change in all other instances of that component. Use the Show Usage command to view all other policies associated with this component.

6.3.4 Hyperlinks

An administrator can incorporate hyperlinks in custom messages to assist in explaining security policies or provide links to software updates to maintain integrity compliance. Hyperlinks are available in several policy components. A VPN hyperlink can be created which can point to either the VPN client executable, or to a batch file which can run and fully log the user in to the VPN (see "VPN Enforcement" on page 95 for more details).

***Figure 6-39** Custom User Message with a Hyperlink*



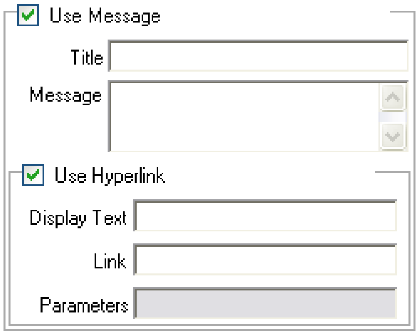
Please Log-In

Please log-in to the VPN

To create a hyperlink, perform the following steps (see Figure 6-40 on page 125 for an example of the control):

1. Enter a name for the link. This is the name that will display below the message (required for Advanced VPN hyperlinks as well).
2. Enter the hyperlink
3. Enter any switches or other parameters for the link (use for VPN enforcement)

Figure 6-40 *Custom Message and Hyperlink Controls*



☑ Use Message

Title

Message

☑ Use Hyperlink

Display Text

Link

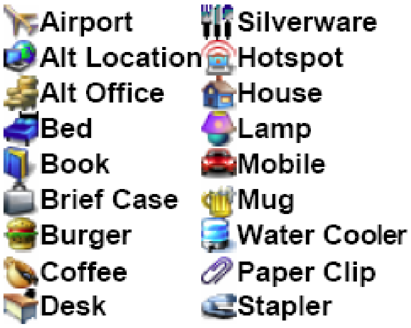
Parameters

NOTE: Changing the Message or Hyperlink in a shared component will change in all other instances of that component. Use the Show Usage command to view all other policies associated with this component.

6.3.5 Defined Location Settings

Setting the Location Icon

The location icon provides a visual cue to the user which identifies their current location. The location icon displays on the taskbar in the notification area. Use the pull-down list to view and select from the available location icons:



Airport
Alt Location
Alt Office
Bed
Book
Brief Case
Burger
Coffee
Desk
Silverware
Hotspot
House
Lamp
Mobile
Mug
Water Cooler
Paper Clip
Stapler

Select an icon which will help the end-user easily identify their location at a glance.

Update Interval

This setting determines the frequency the Endpoint Security Client will check for a policy update when it enters this location. The frequency time is set in minutes, hours, or days. Unchecking this parameter means the Endpoint Security Client will NOT check for an update at this location.

User Permissions

User permissions within a location include:

- **Change Location -** this permits the end-user to change to and out of this location. For non-managed locations (i.e., hot-spots, airports, hotels, etc.), this permission should be granted. In controlled environments, where the network parameters are known, this permission can be disabled. The user will NOT be able to switch to, or out of any locations when this permission is disabled, rather the Endpoint Security Client will rely on the network environment parameters entered for this location
- **Change Firewall Settings -** this allows the user to change their firewall settings
- **Save Network Environment -** this allows the user to save the network environment to this location, to permit automatic switching to the location when the user returns. Recommended for any locations the user will need to switch to. Multiple network environments may be saved for a single location. For example, if a Location defined as Airport is part of the current policy, each airport visited by the user can be saved as a network environment for this location. This way, a mobile user can return to a saved airport environment, and the Endpoint Security Client will automatically switch to the Airport location, and apply the defined security settings. A user may, of course, change to a location and not save the environment.
- **Show Location in Client Menu -** this setting allows the location to display in the client menu. If this is unchecked, the location will not display at any time.

Use Location Message

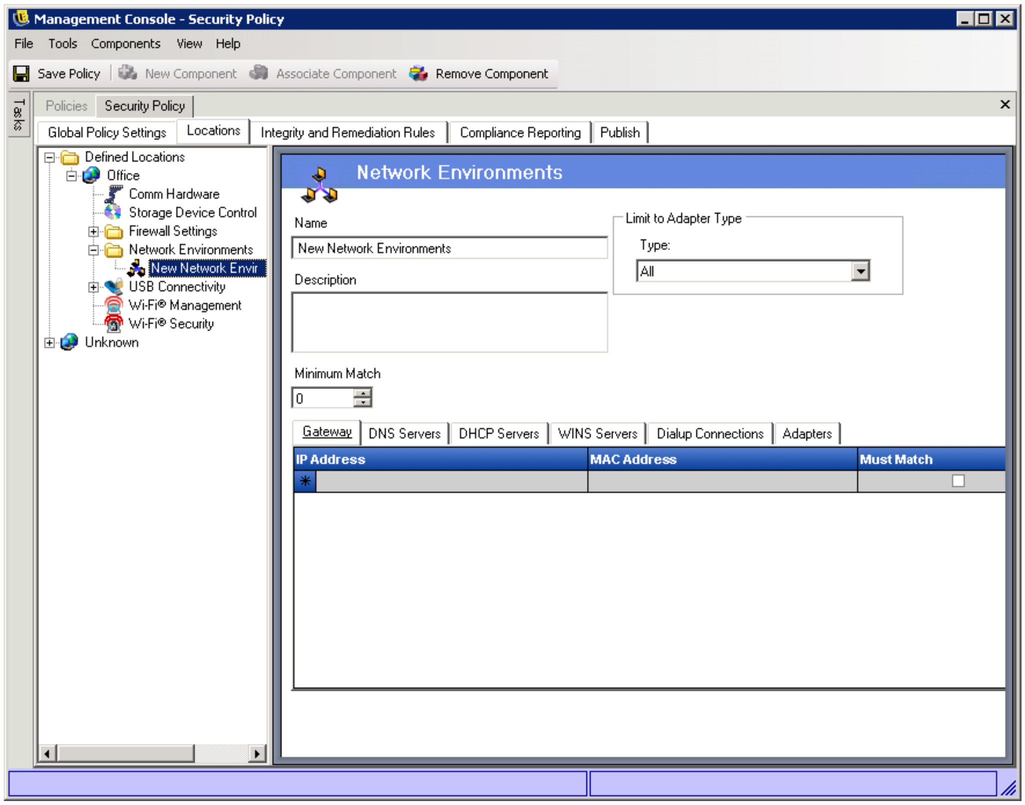
This setting allows an optional Custom User Message to display when the Endpoint Security Client switches to this location. This message can provide instructions for the end-user, details about policy restrictions under this location, or include a Hyperlink to more information.

6.3.6 Network Environments

If the network parameters (Gateway server(s), DNS server(s), DHCP server(s), WINS server(s), available access points, and/or specific adapter connections) are known for a location, the service details (IP and/or MAC), which identify the network, can be entered into the policy to provide immediate location switching without requiring the user having to save the environment as a location.

To access this control, open the Locations tab and click the Network Environments folder in the policy tree on the left.

Figure 6-41 Network Environments



Name: New Network Environments

Description:

Type: All

Minimum Match: 0

IP Address	MAC Address	Must Match
*		☐

The lists provided allow the administrator to define which network services are present in the environment. Each network service may contain multiple addresses. The administrator determines how many of the addresses are required to match in the environment to activate the location switch.

It is required that 2 or more location parameters be used in each network environment definition.

To define a network environment, perform the following steps:

1. Select Network Environments in the components tree and click the New Component button
2. Name the network environment and provide a description
3. Select which adapter type is permitted to access this Network Environment from the drop-down list
4. Enter the following information for each service:
   - The IP address(es) - Limited to 15 characters, and only containing the numbers 0-9 and periods (example: 123.45.6.789)
   - MAC address(es) (Optional) - Limited to 12 characters, and only containing the numbers 0-9 and the letters A-F (upper and lower case); separated by colons example: 00:01:02:34:05:B6
   - Check whether identification of this service is required to define the network environment

5 The Dialup Connections, and Adapters tabs have the following requirements:

- For Dialup Connections, the RAS Entry name from the phone book or the dialed number may be entered. Phone book entries MUST contain alpha characters and cannot contain only special characters (@, #, $,%, -, etc.) or numeric characters (1-9). Entries that only contain special and numeric characters are assumed to be dialed numbers.
- Adapters can be entered to restrict exactly which adapters, specifically, are permitted access to this network environment (see Step 3 regarding setting adapter limitations). Enter the SSID for each allowed adapter. If no SSIDs are entered, all adapters of the permitted type are granted access

6 Each Network Environment has a minimum number of addresses the Endpoint Security Client uses to identify it. The number set in Minimum Match must not exceed the total number of network addresses identified as being required in the tabbed lists. Enter the minimum number of network services required to identify this network environment

To associate an existing Network Environment to this location:

1. Select Network Environments in the components tree and click the Associate Component button
2. Select the network environment from the list
3. The environment parameters may be re-defined. However, changing the settings in a shared component will affect all other instances of this same component. Use the Show Usage command to view all other policies associated with this component.
4. Click Save

You can associate additional Network Environments to the location if desired. If you have multiple locations in the same security policy, be aware that associating a single network environment to two or more locations within in the same security policy will cause unpredictable results and is not recommended.

6.3.7 Firewall Settings

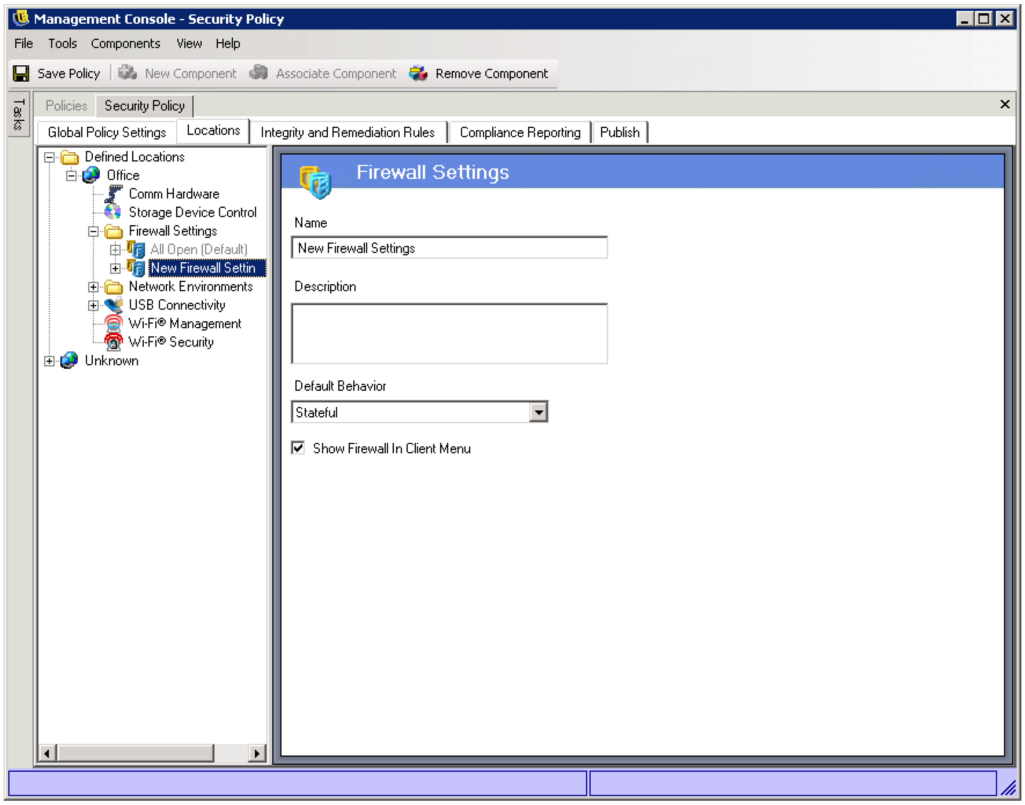
Firewall Settings control the connectivity of all networking ports, Access Control lists, network packets (ICMP, ARP, etc.), and which applications are permitted to get a socket out or function, when the firewall setting is applied.

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for UWS security policies.

To access this control, open the Locations tab and click the Firewall Settings icon in the policy tree on the left.

Each component of a firewall setting is configured separately, with only the default behavior of the TCP/UDP ports required to be set. This setting affects all TCP /UDP ports when this firewall setting is used. Individual or grouped ports may be created with a different setting.

Figure 6-42 *Firewall Settings*



Name: New Firewall Settings

Description:

Default Behavior: Stateful

☑ Show Firewall In Client Menu

To create a new firewall setting:

1. Select Firewall Settings in the components tree and click the New Component button
2. Name the firewall setting and provide a description
3. Select the default behavior for all TCP/UDP ports

   Additional ports and lists may be added to the firewall settings, and given unique behaviors which will override the default setting.

   Example: The default behavior for all ports is set as All Stateful. The ports lists for Streaming Media and Web Browsing are added to the firewall setting. The Streaming Media port behavior is set as Closed, and the Web Browsing port behavior is set as Open. Network traffic through TCP Ports 7070, 554, 1755, and 8000 would be blocked. Network traffic through ports 80 and 443 would be open and visible on the network. All other ports would operate in Stateful mode, requiring the traffic through them be solicited first.
4. Select whether to display this firewall in the Endpoint Security Client menu (if unchecked, the user will not see this firewall setting)
5. Click Save. Repeat the above steps to create another firewall setting

To associate an existing firewall setting:

1. Select Firewall Settings in the components tree and click the Associate Component button
2. Select the desired firewall setting(s) from the list

3. The default behavior setting may be re-defined. However, cChanging the settings in a shared component will affect all other instances of this same component. Use the Show Usage command to view all other policies associated with this component.
4. Click Save

Multiple firewall settings can be included within a single location. One is defined as the default setting, with the remaining settings available as options for the user to switch to. Having multiple settings are useful when a user may normally need certain security restrictions within a network environment and occasionally needs those restrictions either lifted or increased for a short period of time, for specific types of networking (i.e., ICMP Broadcasts).

Three firewall settings are included at installation, they are:

- **All Adaptive -** This firewall setting sets all networking ports as stateful (all unsolicited inbound network traffic is blocked. All outbound network traffic is allowed), ARP and 802.1x packets are permitted, and all network applications are permitted a network connection, all.
- **All Open -** This firewall setting sets all networking ports as open (all network traffic is allowed), all packet types are permitted. All network applications are permitted a network connection
- **All Closed -** This firewall setting closes all networking ports, and restricts all packet types.

A new location will have the single firewall setting, All Open, set as the default. To set a different firewall setting as the default, right click the desired Firewall Setting and choose Set as Default.

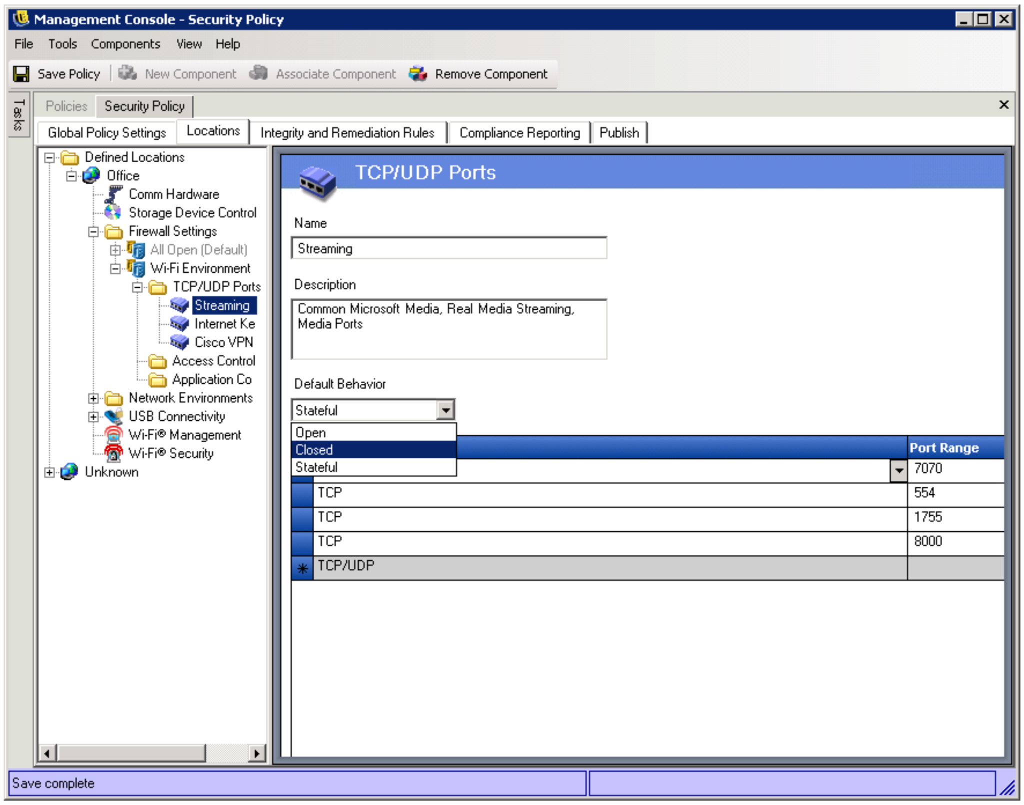
6.3.8 TCP/UDP Ports

Endpoint data is primarily secured by controlling TCP/UDP port activity. This feature allows you to create a list of TCP/UDP ports which will be uniquely handled in this firewall setting. The lists contain a collection of ports and port ranges, together with their transport type, which defines the function of the range.

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for UWS security policies.

To access this control, open the Locations tab, click the “+” symbol next to Firewall Settings, click the “+” symbol next to the desired Firewall, and click the TCP/UDP Ports icon in the policy tree on the left.

Figure 6-43 *TCP/UDP Ports Settings*



Name: Streaming

Description: Common Microsoft Media, Real Media Streaming, Media Ports

Default Behavior: Stateful

	Port Range
	7070
TCP	554
TCP	1755
TCP	8000
TCP/UDP	

Save complete

New TCP/UDP port lists can be defined with individual ports or as a range (1-100) per each line of the list.

To create a new TCP/UDP port setting:

1. Select TCP/UDP Ports from the components tree and click the Add New button
2. Name the port list and provide a description
3. Select the port behavior from the drop-down list. The optional behaviors are:
   - **Open** - All network inbound and outbound traffic is allowed. Because all network traffic is allowed your computer identity is visible for this port or port range.
   - **Closed** - All inbound and outbound network traffic is blocked. Because all network identification requests are blocked your computer identity is concealed for this port or port range.
   - **Stateful** - All unsolicited inbound network traffic is blocked. All outbound network traffic is allowed over this port or port range.
4. Enter the transport type:
   - All (all port types listed below)
   - Ether
   - IP
   - TCP
   - UDP

5. Enter Ports and Port Ranges as either:
   - Single ports
   - A range of ports with the first port number, followed by a dash, and the last port number

     Example: 1-100 would add all ports between 1 and 100

     Please visit the Internet Assigned Numbers Authority pages (http://www.iana.org) for a complete Ports and transport types list.

Click Save. Repeat the above steps to create a new setting

To associate an existing TCP/UDP port to this firewall setting:

1. Select TCP/UDP Ports from the component tree and click the Associate Component button
2. Select the desired port(s) from the list
3. The default behavior setting may be re-defined. However, changing the settings in a shared component will affect ALL OTHER instances of this same component. Use the Show Usage command to view all other policies associated with this component.
4. Click Save

Several TCP/UDP port groups have been bundled and are available at installation:

Name	Description	Transport	Value
All Ports	All Ports	All	1-65535
BlueRidge VPN	Ports used by the BlueRidge VPN Client	UDP	820
Cisco VPN	Ports used by the Cisco VPN Client	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524
Common Networking	Commonly required Networking Ports for building firewalls	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847

Name	Description	Transport	Value
Database Communication	Microsoft, Oracle, Siebel, Sybase, SAP Database Ports	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
File Transfer Protocol (FTP)	File Transfer Protocol Port	TCP/UDP	21
Instant Messaging	Microsoft, AOL, Yahoo Instant Messaging Ports	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
Internet Key Exchange Compatible VPN	Ports used by Internet Key Exchange Compatible VPN Clients	UDP	500
Microsoft Networking	Common File Sharing / Active Directory Ports	TCP/UDP	135-139, 445
Open Ports	Ports that are opened for this firewall	TCP/UDP	80
Streaming Media	Common Microsoft/Real Streaming Media Ports	TCP	7070, 554, 1755, 8000
Web Browsing	Common Web Browser Ports, including SSL	All	80, 443

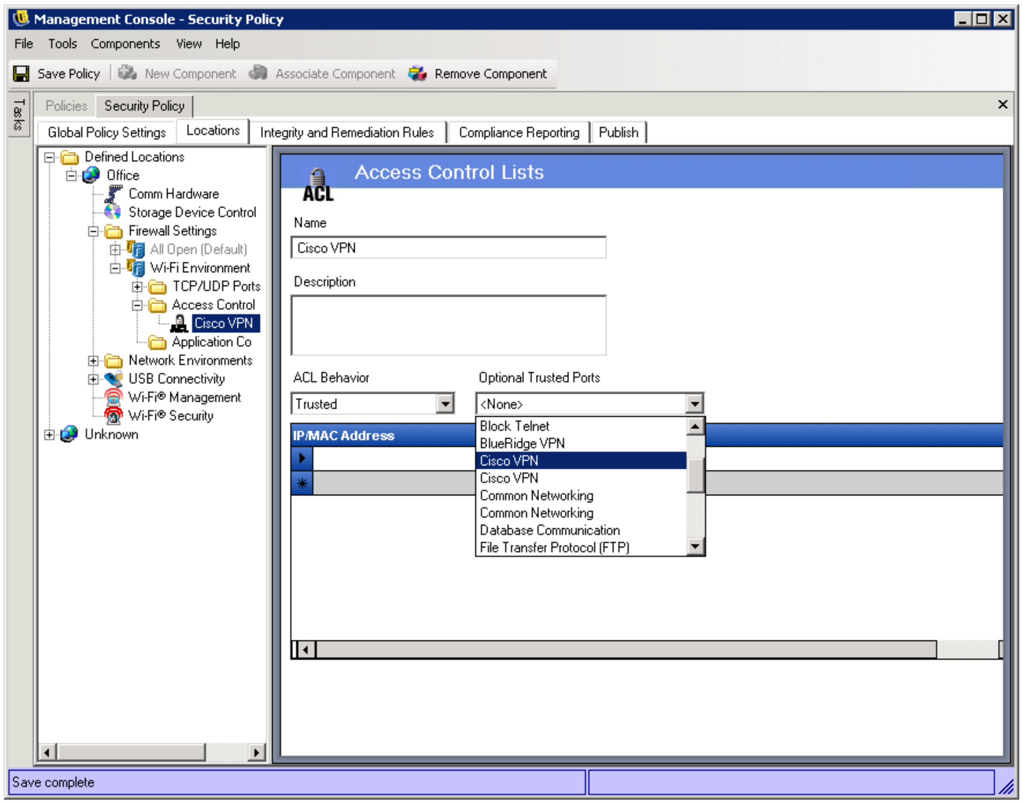
6.3.9 Access Control Lists

There may be some addresses which require unsolicited traffic be passed regardless of the current port behavior (i.e., enterprise back-up server, exchange server, etc.). In instances where unsolicited traffic needs to be passed to and from trusted servers, an Access Control List (ACL) can be created to resolve this issue.

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for UWS security policies.

To access this control, open the Locations tab, click the "+" symbol next to Firewall Settings, click the "+" symbol next to the desired Firewall, and click the Access Control Lists icon in the policy tree on the left.

Figure 6-44 *Access Control Lists Settings*



Name: Cisco VPN

Description:

ACL Behavior: Trusted

Optional Trusted Ports: <None>

To create a new ACL setting:

1. Select Access Control List from the components tree and click the Add New button
2. Name the ACL and provide a description
3. Enter the ACL address or Macro
4. Enter the ACL type:
   - **IP -** This type limits the address to 15 characters, and only containing the numbers 0-9 and periods (example: 123.45.6.189). IP addresses may also be entered as a range (example: 123.0.0.0 - 123.0.0.255)

- **MAC -** This type limits the address to 12 characters, and only containing the numbers 0-9 and the letters A-F (upper and lower case); separated by colons (example: 00:01:02:34:05:B6)

5. Select the ACL Behavior drop-down box and determine whether the ACLs listed should be Trusted (allow it always even if all TCP/UDP ports are closed) or Non-Trusted (block access)
6. If Trusted, select the Optional Trusted Ports (TCP/UDP) this ACL will use. These ports will permit all ACL traffic, while other TCP/UDP ports will maintain their current settings. Selecting ‹None› means any port may be used by this ACL
7. Click Save. Repeat the above steps to create a new setting

To associate an existing ACL/Macro to this firewall setting:

1. Select Access Control List from the component tree and click the Associate Component button
2. Select the ACL(s)/Macro(s) from the list
3. The ACL behavior settings may be re-defined. However, changing the settings in a shared component will affect ALL OTHER instances of this same component. Use the Show Usage command to view all other policies associated with this component.
4. Click Save

Network Address Macros List

The following is a list of special Access Control macros. These can be associated individually as part of an ACL in a firewall setting.

Table 6-1 *Network Address Macros*

Macro	Description
[Arp]	Allow ARP (Address Resolution Protocol) packets. The term Address Resolution refers to the process of finding an address of a computer in a network. The address is Resolved using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.
[Icmp]	Allow ICMP (Internet Control Message Protocol) packets. ICMPs are used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.
[IpMulticast]	Allow IP Multicast packets. Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. Multicast packets may be distributed using either IP or Ethernet addresses.

Macro	Description
[EthernetMulticast]	Allow Ethernet Multicast packets.
[IpSubnetBrdcast]	Allow Subnet Broadcast packets. Subnet broadcasts are used to send packets to all hosts of a subnetted, supernetted, or otherwise nonclassful network. All hosts of a nonclassful network listen for and process packets addressed to the subnet broadcast address.
[Snap]	Allow Snap encoded packets.
[LLC]	Allow LLC encoded packets.
[Allow8021X]	Allow 802.1x packets. To overcome deficiencies in Wired Equivalent Privacy (WEP) keys, Microsoft and other companies are utilizing 802.1x as an alternative authentication method. 802.1x is a port-based, network access control, which uses Extensible Authentication Protocol (EAP), or certificates. Currently, most major wireless card vendors and many access point vendors support 802.1x. This setting also allows Light Extensible Authentication Protocol (LEAP) and WiFi Protected Access (WPA) authentication packets.
[Gateway]	Represents the current IP configuration Default Gateway address. When this value is entered, the Endpoint Security Client allows all network traffic from the current IP configuration Default Gateway as a trusted ACL.
[GatewayAll]	Same as [Gateway] but for ALL defined gateways.
[Wins]	Represents current client IP configuration Default WINS Server address. When this value is entered, the Endpoint Security Client allows all network traffic from the current IP configuration Default WINS server as a trusted ACL.
[WinsAll]	Same as [Wins] but for ALL defined WINS servers.
[Dns]	Represents current client IP configuration Default DNS server address. When this value is entered, the Endpoint Security Client allows all network traffic from the current IP configuration Default DNS server as a trusted ACL.
[DnsAll]	Same as [Dns] but for ALL defined DNS servers.
[Dhcp]	Represents current client IP configuration Default DHCP server address. When this value is entered, the Endpoint Security Client allows all network traffic from the current IP configuration Default DHCP server as a trusted ACL.
[DhcpAll]	Same as [Dhcp] but for ALL defined DHCP servers.

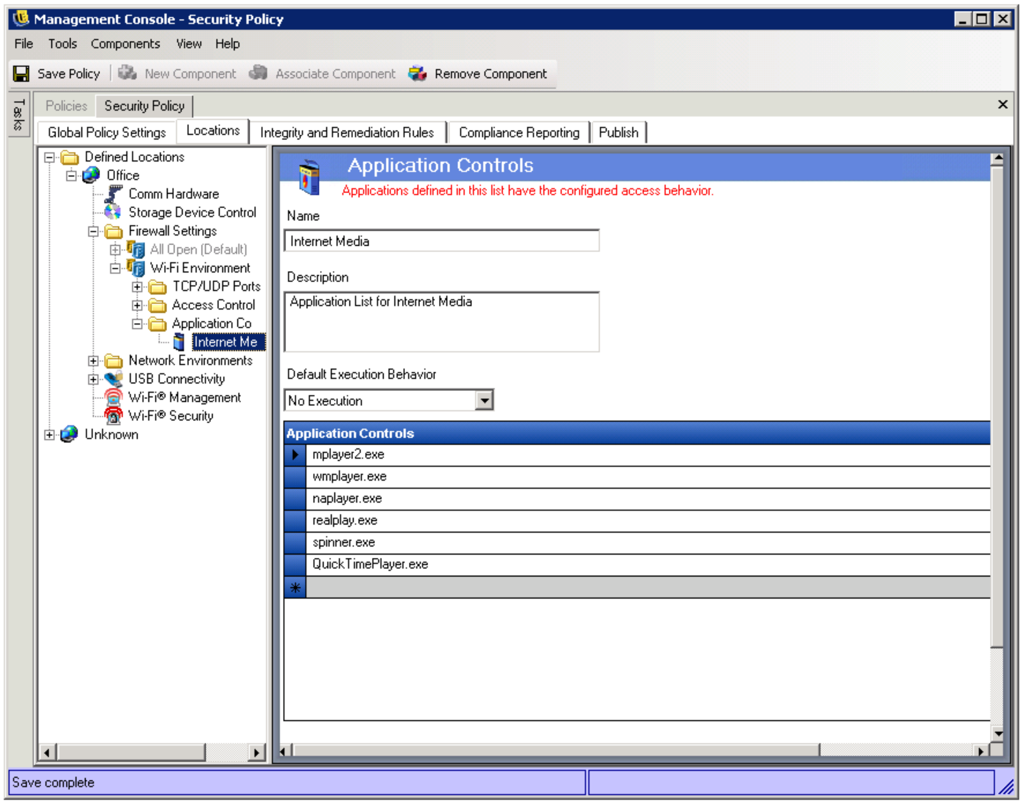
6.3.10 Application Controls

This feature allows the administrator to block applications either from gaining network access, or from simply executing at all.

NOTE: This feature is only available in the ZENworks Endpoint Security Management installation, and cannot be used for UWS security policies.

To access this control, open the Locations tab, click the “+” symbol next to Firewall Settings, click the “+” symbol next to the desired Firewall, and click the Applications Controls icon in the policy tree on the left.

Figure 6-45 Application Control Settings



Applications defined in this list have the configured access behavior.

Name: Internet Media

Description: Application List for Internet Media

Default Execution Behavior: No Execution

Application Controls
mplayer2.exe
wmplayer.exe
naplayer.exe
realplay.exe
spinner.exe
QuickTimePlayer.exe

Save complete

To create a new application control setting:

1. Select Application Controls in the components tree and click the Add New button
2. Name the application control list and provide a description
3. Select an execution behavior. This behavior will be applied to all applications listed. If multiple behaviors are required (example: some networking applications are denied network access, while all file sharing applications are denied execution), multiple application controls will need to be defined. Select one of the following:
   - **All Allowed** - all applications listed will be permitted to execute and have network access
   - **No Execution** - all applications listed will not be permitted to execute
   - **No Network Access** - all applications listed will be denied network access. Applications (such as web-browsers) launched from an application will also be denied network access

   NOTE: Blocking network access for an application does not affect saving files to mapped network drives. Users will be permitted to save to all network drives available to them.
4. Enter each application to block. One application must be entered per row

   WARNING: Blocking execution of critical applications could have an adverse affect on system operation. Blocked Microsoft Office applications will attempt to run their installation program.
5. Click Save. Repeat the above steps to create a new setting

To associate an existing application control list to this firewall setting:

1. Select Application Controls in the components tree and click the Associate Component button
2. Select an application set from the list
3. The applications and the level of restriction may be re-defined

   NOTE: Changing the settings in a shared component will affect ALL OTHER instances of this same component. Use the Show Usage command to view all other policies associated with this component.

4. Click Save

The available application controls are identified below, the default execution behavior is No Network Access:

Table 6-2 *Application Controls*

Name	Applications
Web Browsers	explore.exe; netscape.exe; netscp.exe
Instant Messaging	aim.exe; icq.exe; msmsgs.exe; msnmsgr.exe; trillian.exe; ypager.exe
File Sharing	blubster.exe; grokster.exe; imesh.exe; kazaa.exe; morpheus.exe; napster.exe; winmx.exe
Internet Media	mplayer2.exe; wmplayer.exe; naplayer.exe; realplay.exe; spinner.exe; QuickTimePlayer.exe

If the same application is added to two different application controls in the same firewall setting (i.e., kazaa.exe is blocked from executing in one application control, and blocked from gaining network access in another defined application control under the same firewall setting), the most stringent control for the given executable will be applied (i.e., kazaa would be blocked from executing)

6.3.11 Rule Scripting Parameters

The ZENworks Endpoint Security Management (ZENworks Endpoint Security Management) supports standard Jscript and VBScript coding methods readily available, with the following exceptions:

1. WScript.Echo - Not supported - (displaying return values back to a parent window are not support (since the parent window is unavailable)). Use the Action.Message ZENworks Endpoint Security Management API instead.
2. Access to Shell Objects - Use the following modified nomenclature/call:

```
[JScript]
   Use:
   var WshShell = new ActiveXObject("WScript.Shell");
   Instead of:
   var WshShell = WScript.CreateObject ("WScript.Shell");

[VBScript]
```

```
Use:
Dim WshShell
Set WshShell = CreateObject("WScript.Shell")
Instead of:
Dim WshShell
Set WshShell = WScript.CreateObject("WScript.Shell")
```

3. All scripts are executed in the "system context" unless the following comment is added to the top of the script:

   ```
   [Jscript]
   //@ImpersonateLoggedOnUser
   [VBScript]
   '@ImpersonateLoggedOnUser
   ```

Rule Scripting

A rule consists of two parts. The first part is the Trigger Events which determine when to execute the rule. The second part is the scripting code which contains the logic of the rule. The Endpoint Security Client provides three namespaces and five interfaces for the script, which allows the script to control or access the client.

The namespaces are as follows:

1. **Query.** This namespace provides methods to get the current state of the client. For example, information about the adapters, shield states and location.
2. **Action.** This namespace provides methods that get the client to do something. For example, a call that puts the client into a quarantined shield state.
3. **Storage.** This namespace provides a mechanism for the script to store variables for the session or permanently. These could be used to tell the script if the rule had failed the last time it was run. It could be used to store when this rule last ran.

The interfaces are as follows:

1. **IClientAdapter.** This interface describes an adapter in the client network environment.
2. **IClientEnvData.** This interface returns environment data about a Server or Wireless Access Point.
3. **IClientNetEnv.** Provides Network Environment Information.
4. **IClientWAP.** Provides information about a Wireless Access Point.
5. **IClientAdapterList.** A list of adapters in the client network environment.

Trigger Events

Triggers are events that cause the Endpoint Security Client to determine when and if a rule should be executed. These events can either be internal to the client or some external event monitored by the client.

- AdapterArrival

  Desc: Adapter arrival has occurred.

  Parameters: None.

- AdapterRemoval

  Desc: Adapter had been removed.

Parameters: None.

- DownloadFailed

  Desc: This event is triggered in response to Action.DownloadAsync if the file was not successfully downloaded.

  Parameters: None.

- DownloadSuccess

  Desc: This event is triggered in response to Action.DownloadAsync if the file was successfully downloaded

  Parameters: None.

- LocationChange

  Desc: Run the rule when entering or leaving a particular location or all locations.

  Parameters:

OldLocation (opt):	Uuid of a Location
NewLocation (opt):	Uuid of a Location
ManualChange(opt):	(true/false). User manually changed location.

- MediaConnect

  Desc: Adapter has connection.

  Parameters: None.

- MediaDisconnect

  Desc: Adapter has lost its connection.

  Parameters: None.

- PolicyUpdated

  Desc: Called when client is first started and whenever a new policy is applied.

  Parameters: None.

- ProcessChange

  Desc: Trigger whenever a process is created or deleted.

  Parameters: None.

- Startup

  Desc: Run the rule when the engine is started.

  Parameters: None.

- TimeOfDay

  Desc: Run the rule at a particular time or times of day. Or at least once a day. This will store the last time this was triggered.

  Parameters:

Time:	HH:MM (Example: 04:00,15:10) Military time. Lowest to highest. Max=5.
Days:	(Sun,Mon,Tue,Wed,Thu,Fri,Sat) One or more. Comma separated.

Type:	(Local/UTC).

- Timer

  Desc: Run the rule every n milliseconds.

  Parameters:

Interval:	Number of milliseconds

- UserChangeShield

  Desc: The user had manually changed the shield state.

  Parameters: None.

- WithinTime

  Desc: Run the rule every n minutes starting from the last time the rule was executed. If the computer has been turned off it will execute the rule if the specified time has past since the last time the rule was executed.

  Parameters:

WithinMinutes:	Number of seconds

Script Namespaces

General Enumerations and File substitutions

```
EAccessState
eApplyGlobalSetting = -1
eDisableAccess = 0
eAllowAccess = 1
EAdapterType
                eWIRED
                eWIRELESS
                eDIALUPCONN
EComparison
                eEQUAL
                eLESS
                eGREATER
                eEQUALORLESS
                eEQUALORGREATER?
ESTDisplayMsg
                eONLYONCE
                eEVERYTIME
                eSECONDS
                eNOMSG
EHardwareDeviceController
eIrDA = 0
e1394
eBlueTooth
eSerialPort
eParrallelPort
ELogLevel
```

```
                eALARM
                eWARN
                eINFO
EMATCHTYPE
                eUNDEFINED
                eLOCALIP
                eGATEWAY
                eDNS
                eDHCP
                eWINS
                eWAP
                eDIALUP
                eUNKNOWN
                eDOMAIN
                eRULE
                eUSERSELECTED
EMinimumWiFiSecurityState
eNoEncryptionRequired = 0
eWEP64
eWEP128
eWPA
ERegKey
                eCLASSES_ROOT
                eCURRENT_USER
                eLOCAL_MACHINE
                eUSERS
                eCURRENT_CONFIG
ERegType
                eSTRING
                eDWORD
                eBINARY
                eMULTI_SZ
                eEXPAND_SZ
EServiceState
                eRUN
                eSTOP
                ePAUSE
                ePENDING
                eNOTREG
EVariableScope
ePolicyChange = 0   // reset on a policy update
eLocationChange = 1   // reset on a location change
TRIGGEREVENT
                eTIMER
                eSTARTUP
                eLOCATIONCHANGE
                eTIMEOFDAY
                eADAPTERARRIVAL
                eADAPTERREMOVAL
                eMEDIACONNECT
                eMEDIADISCONNECT
                ePOLICYUPDATED
                eUSERCHANGEDSHIELD
                ePROCESSCHANGE
                eWITHINTIME
                eRUNNOW
                eDOWNLOADFAILED
                eDOWNLOADSUCCESS
```

Table 6-3 Shell Folder Names

%windows%	C:\Windows
%system%	%windows%\System32
%startup%	%programs%\Startup
%startmenu%	%profile%\Start Menu
%programs%	%startmenu%\Programs
%commonprogramfiles%	%programfiles%\Common
%programfiles%	C:\Program Files
%profile%	C:\Documents and Settings\username
%localappdata%	%profile%\Local Settings\Application Data
%appdata%	%profile%\Application Data
%commonappdata%	C:\Documents and Settings\All Users\Application Data
%commonprograms%	C:\Documents and Settings\All Users\Start Menu\Programs
%cookie%	%profile%\Cookies

Action Namespace

CheckForUpdate

JScript:

```
Action.CheckForUpdate();
```

VBScript:

```
Action.CheckForUpdate()
```

ClearFixedShieldState, SetShieldStateByName, Trace, Sleep

NOTE: When setting the ShieldState (firewall) by name, the name specified MUST EXACTLY match the firewall specified in the policy. Three firewall settings are always available regardless of the policy ("All Closed", "All Adaptive", and "All Open").

JScript:

```
   Action.SetShieldStateByName("Closed",true);
   Action.Trace("Start 20 second sleep");
   Action.Sleep(20000);
   var ret = Action.ClearFixedShieldState();
   if(ret == true)
     Action.Trace("ret = true");
   else
     Action.Trace("ret = false");
```

VBScript:

```
   Action.SetShieldStateByName "Closed",true
   Action.Trace("Start 20 second sleep")
   Action.Sleep(20000)
   dim ret
   ret = Action.ClearFixedShieldState()
   if(ret = true) then
     Action.Trace("ret = true")
   else
     Action.Trace("ret = false")
   end if
```

ClearStamp, SwitchLocationByName, Stamp

NOTE: When setting the Location by name, the name specified MUST EXACTLY match the location specified in the policy.

JScript:

```
   Action.SwitchLocationByName("Base");
   Action.Stamp();
   Action.Trace("Begin 20 second sleep");
   Action.Sleep(20000);
   Action.SwitchLocationByName("Base");
   Action.ClearStamp();
```

VBScript:

```
   Action.SwitchLocationByName("Base")
   Action.Stamp()
   Action.Trace("Begin 20 second sleep")
   Action.Sleep(20000)
   Action.SwitchLocationByName("Base")
   Action.ClearStamp()
```

Details:

Base must be the name of a valid location which can be stamped. This script will then switch to location Base, then stamp it, sleep for 20 seconds, make sure we didn't spin out of the location by switching back to base and then clear the stamp. This script performed all actions as expected.

CreateRegistryKey

JScript:

```
   var ret = 
Action.CreateRegistryKey(eLOCAL_MACHINE,"Software\\Novell","Tester");
   if(ret == true)
     Action.Trace("Create Key is Successful");
   else
     Action.Trace("Create Key did not work");
```

VBScript:

```
dim ret
   ret = Action.CreateRegistryKey(eLOCAL_MACHINE,"Software\\Novell","Tester")
   if(ret = true) then
     Action.Trace("Create Key is Successful")
   else
     Action.Trace("Create Key did not work")
   end if
```

DeleteRegistryKey

JScript:

```
   var ret = 
Action.DeleteRegistryKey(eLOCAL_MACHINE,"Software\\Novell\\Tester");
   if(ret == true)
     Action.Trace("Delete Key is Successful");
   else
     Action.Trace("Delete Key did not work");
```

VBScript:

```
   dim ret
   ret = Action.DeleteRegistryKey(eLOCAL_MACHINE,"Software\\Novell\\Tester")
   if(ret = true) then
     Action.Trace("Delete Key is Successful")
   else
     Action.Trace("Delete Key did not work")
   end if
```

DeleteRegistryValue

JScript:

```
Action.DeleteRegistryValue(eLOCAL_MACHINE,"Software\\Novell\\Tester","val1");

Action.DeleteRegistryValue(eLOCAL_MACHINE,"Software\\Novell\\Tester","val2");
```

VBScript:

```
   Action.DeleteRegistryValue eLOCAL_MACHINE,"Software\\Novell\\Tester","val1"
   Action.DeleteRegistryValue eLOCAL_MACHINE,"Software\\Novell\\Tester","val2"
```

DisplayMessage, DisplayMessageByName

NOTE: The first parameter of the DisplayMessage call is a unique integer identifier for each action. When calling the Message by name, the name specified MUST EXACTLY match the DisplayMessage specified in the policy.

JScript:

```
   Action.DisplayMessage("40","Message40", "Message Here", "question", "");
   Action.Sleep(10000);
   Action.DisplayMessageByName("Message40");
```

VBScript:

```
Action.DisplayMessage "40","Message40", "Message Here", "question", ""
Action.Sleep(10000)
Action.DisplayMessageByName "Message40"
```

Details:

This script will create a Message Box with all parameters and then wait 10 seconds, (during which the tester should click Ok to end box display) and then it will be displayed by the ID and wait 10 seconds, (again, the tester should click Ok to end box display) and then it will display the Message Box by

EnableAdapterType

JScript:

```
Action.EnableAdapterType(false, eWIRELESS);
Action.EnableAdapterType(true, eWIRELESS);
Action.EnableAdapterType(false, eWIRED);
Action.EnableAdapterType(true, eWIRED);
Action.EnableAdapterType(false, eDIALUPCONN);
Action.EnableAdapterType(true, eDIALUPCONN);
```

VBScript:

```
Action.EnableAdapterType false, eWIRELESS
Action.EnableAdapterType true, eWIRELESS
Action.EnableAdapterType false, eWIRED
Action.EnableAdapterType true, eWIRED
Action.EnableAdapterType false, eDIALUPCONN
Action.EnableAdapterType true, eDIALUPCONN
```

Launch

NOTE: The first parameter of the Launch call is a unique integer identifier for each action.

JScript:

```
Action.Launch("50","C:\calco.exe","");
```

VBScript:

```
Action.Launch "51","C:\calco.exe",""
```

LaunchAsSystem

JScript:

```
Action.LaunchAsSystem("C:\calco.exe"," sParameters ", "sWorkingDir",true);
```

VBScript:

```
Action.LaunchAsSystem "C:\calco.exe"," sParameters"," sWorkingDir",true
```

LaunchAsUserWithCode

This launches in the user context and returns the exit code of the application launched.

JScript:

```
Action.LaunchAsUserWithCode(appToLaunch, "sParameters", "sWorkingDir", bShow,
bWait, nExitCode);
```

VBScript:

```
Action.LaunchAsUserWithCode appToLaunch, "sParameters", "sWorkingDir", bShow,
bWait, nExitCode
```

Details:

Preliminary setup required creating a policy which included a new Integrity rule with a custom message. The custom message included a launch link which was added to the SCC menu bar.

LaunchLinkByName

NOTE: When setting the LaunchLink by name, the name specified MUST EXACTLY match the launch link specified in the policy.

JScript:

```
   Action.LaunchLinkByName("MyLink");
```

VBScript:

```
   Action.LaunchLinkByName "MyLink"
```

LogEvent

JScript:

```
   Action.LogEvent("MyEvent", eALARM, "This is a log test message");
```

VBScript:

```
   Action.LogEvent "MyEvent", eALARM, "This is a vb log test message"
```

Details:

Pre-requisite is that logging needs to be enabled.

Message

Asynchronous Message (displayed and script continues):

JScript:

```
Action.Message("Display sync message");
```

VBScript:

```
Action.Message "Display sync message"
```

Synchronous Message (displayed and waits for user respond before the script continues):

NOTE: nTimeoutSeconds values of -1 or 0 will NEVER timeout nMessageType (buttons shown):

1. Ok/Cancel
2. Abort/Retry/Ignore
3. Yes/No/Cancel

Currently, the return value which of these buttons pressed by the user is NOT returned, so it is NOT helpful for conditional logic control.

JScript:

```
Action.Message("Message Title Bar", nMessageType, nTimeoutSeconds);
```

VBScript:

```
Action.Message "Message Title Bar", nMessageType, nTimeoutSeconds
```

PauseService

JScript:

```
Action.PauseService("lanmanworkstation");
```

VBScript:

```
Action.PauseService "lanmanworkstation"
```

Details:

Make sure you use the actual service name, not the display name.

Prompt

This API creates dialog boxes and user interfaces. It will be covered in a future revision given the complexity and need for examples.

StartService

JScript:

```
Action.StartService("lanmanworkstation","");
```

VBScript:

```
Action.StartService "lanmanworkstation",""
```

Details:

Make sure you use the actual service name, not the display name.

StopService

JScript:

```
Action.StopService("lanmanworkstation");
```

VBScript:

```
Action.StopService "lanmanworkstation"
```

Details:

Make sure you use the actual service name, not the display name.

WriteRegistryDWORD, WriteRegistryString

JScript:

```
      var ret = 
Action.CreateRegistryKey(eLOCAL_MACHINE,"Software\\Novell","Tester");
      if(ret == true)
        Action.Trace("Create Key is Successful");
      else
        Action.Trace("Create Key did not work");
Action.WriteRegistryDWORD(eLOCAL_MACHINE,"Software\\Novell\\Tester","val1",24
);
Action.WriteRegistryString(eLOCAL_MACHINE,"Software\\Novell\\Tester","val2","
Novell");
```

VBScript:

```
dim ret
ret = Action.CreateRegistryKey(eLOCAL_MACHINE,"Software\\Novell","Tester")
if(ret = true) then
  Action.Trace("Create Key is Successful")
else
  Action.Trace("Create Key did not work")
end if

Action.WriteRegistryDWORD eLOCAL_MACHINE,"Software\\Novell\\Tester","val1",24
Action.WriteRegistryString 
eLOCAL_MACHINE,"Software\\Novell\\Tester","val2","Novell"
```

Query Namespace, FileExistsVersion

JScript:

```
var ret;
ret = Query.FileExistsVersion("C:","ocalco.exe",eEQUAL,"5","1","2600","0");
if(ret == 1)
  Action.Trace("File is Equal");
else
  Action.Trace("File is Not Equal");
```

VBScript:

```
dim ret
ret = Query.FileExistsVersion("C:\","ocalco.exe",eEQUAL,"5","1","2600","0")
if(ret = true) then
  Action.Trace("File is Equal")
else
  Action.Trace("File is Not Equal")
end if
```

NOTE: Not all files have file version information.

Script as above performed correctly.

GetAdapters

JScript:

```
var adplist;
var adplength;
var adp;

adplist = Query.GetAdapters();
adplength = adplist.Length;

Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
  adp = adplist.Item(0);
  Action.Trace("DeviceID = " + adp.DeviceID);
  Action.Trace("Enabled = " + adp.Enabled);
  Action.Trace("IP = " + adp.IP);
  Action.Trace("MAC = " + adp.MAC);
  Action.Trace("MaxSpeed = " + adp.MaxSpeed);
  Action.Trace("Name = " + adp.Name);
  Action.Trace("SubNetMask = " + adp.SubNetMask);
  Action.Trace("Type = " + adp.Type);
}
```

VBScript:

```
dim adplist
dim adplength
dim adp

set adplist = Query.GetAdapters()
adplength = CInt(adplist.Length)

Action.Trace("adplength = " & adplength)

if(adplength > 0) then
  set adp = adplist.Item(0)
  Action.Trace("DeviceID = " & adp.DeviceID)
  Action.Trace("Enabled = " & adp.Enabled)
  Action.Trace("IP = " & adp.IP)
  Action.Trace("MAC = " & adp.MAC)
  Action.Trace("MaxSpeed = " & CLng(adp.MaxSpeed))
  Action.Trace("Name = " & adp.Name)
  Action.Trace("SubNetMask = " & adp.SubNetMask)
  Action.Trace("Type = " & adp.Type)
end if
```

Details:

This script will get a list of adapters, the length of the list (number of adapters) and enumerate the properties of the first index in the list.

GetCheckinTime

JScript:

```
var ret;
ret = Query.GetCheckinTime();
Action.Trace("LastCheckIn = " + ret);
```

VBScript:

```
dim ret
ret = Query.GetCheckinTime()
Action.Trace("LastCheckIn = " & ret)
```

GetLocationMatchData, LocationMatchCount

JScript:

```
var envdata;
var envdatalength;

envdatalength = Query.LocationMatchCount;

Action.Trace("MatchCount = " + envdatalength);

if(envdatalength > 0)
{
  envdata = Query.GetLocationMatchData(0);
  Action.Trace("IP = " + envdata.IP);
  Action.Trace("MAC = " + envdata.MAC);
  Action.Trace("SSID = " + envdata.SSID);
  Action.Trace("Type = " + envdata.Type);
}
```

VBScript:

```
dim envdata
dim envdatalength

envdatalength = Query.LocationMatchCount

Action.Trace("MatchCount = " & envdatalength)

if(envdatalength > 0) then
  set envdata = Query.GetLocationMatchData(0)
  Action.Trace("IP = " & envdata.IP)
  Action.Trace("MAC = " & envdata.MAC)
  Action.Trace("SSID = " & envdata.SSID)
  Action.Trace("Type = " & envdata.Type)
end if
```

Details:

This script requires an environment to be defined for a location in the policy in order to provide useful data. This script will then get the Location Match Count and if it is greater than 0, then it will enumerate the attributes for the first Location Match Data.

IsAdapterTypeConnected

JScript:

```
var ret;
ret = Query.IsAdapterTypeConnected(eWIRED);
Action.Trace("IsWiredConnected = " + ret);
ret = Query.IsAdapterTypeConnected(eWIRELESS);
Action.Trace("IsWirelessConnected = " + ret);
ret = Query.IsAdapterTypeConnected(eDIALUPCONN);
Action.Trace("IsModemConnected = " + ret);
```

VBScript:

```
dim ret
ret = Query.IsAdapterTypeConnected(eWIRED)
Action.Trace("IsWiredConnected = " & ret)
ret = Query.IsAdapterTypeConnected(eWIRELESS)
Action.Trace("IsWirelessConnected = " & ret)
ret = Query.IsAdapterTypeConnected(eDIALUPCONN)
Action.Trace("IsModemConnected = " & ret)
```

IsAuthenticated

JScript:

```
var ret = Query.IsAuthenticated();
Action.Trace("Is authenticated = " + ret);
```

VBScript:

```
dim ret
ret = Query.IsAuthenticated()
Action.Trace("Is authenticated = " & ret)
```

IsWindowsXP

JScript:

```
var ret = Query.IsWindowsXP();
Action.Trace("Is XP = " + ret);
```

VBScript:

```
dim ret
ret = Query.IsWindowsXP()
Action.Trace("Is XP = " & ret)
```

IsWindows2000

JScript:

```
var ret = Query.IsWindows2000();
Action.Trace("Is Win2000 = " + ret);
```

VBScript:

```
dim ret
ret = Query.IsWindows2000()
Action.Trace("Is Win2000 = " & ret)
```

ProcessIsRunning

JScript:

```
var ret = Query.ProcessIsRunning("STEngine.exe",eEQUAL,"","","","");
Action.Trace("Is Running = " + ret);
```

VBScript:

```
dim ret
ret = Query.ProcessIsRunning("STEngine.exe",eEQUAL,"","","","")
Action.Trace("Is Win2000 = " & ret)
```

RegistryKeyExists

JScript:

```
var ret;
ret = Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell");
Action.Trace("Reg Key Exists = " + ret);
```

VBScript:

```
dim ret
ret = Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell")
Action.Trace("Reg Key Exists = " & ret)
```

RegistryValueDWORD

JScript:

```
      var ret;
      ret = 
Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell\\Logging");
      Action.Trace("Reg Key Exists = " + ret);

      ret = 
Query.RegistryValueDWORD(eLOCAL_MACHINE,"Software\\Novell\\Logging","Enabled"
);
      Action.Trace("Reg Value = " + ret);
```

VBScript:

```
      dim ret
      ret = Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\Novell\Logging")
      Action.Trace("Reg Key Exists = " & ret)

      ret = 
Query.RegistryValueDWORD(eLOCAL_MACHINE,"Software\Novell\Logging","Enabled")
      Action.Trace("Reg Value = " & CLng(ret))
```

RegistryValueExists

JScript:

```
        var ret;
        ret =
Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell\\Logging");
        Action.Trace("Reg Key Exists = " + ret);

        ret =
Query.RegistryValueExists(eLOCAL_MACHINE,"Software\\Novell\\Logging","Enabled
",eDWORD);
        Action.Trace("Reg Value Exists = " + ret);
```

VBScript:

```
        dim ret
        ret =
Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell\\Logging")
        Action.Trace("Reg Key Exists = " & ret)

        ret =
Query.RegistryValueExists(eLOCAL_MACHINE,"Software\\Novell\\Logging","Enabled
",eDWORD)
        Action.Trace("Reg Value Exists = " & ret)
```

RegistryValueString

JScript:

```
var ret;
ret = Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell\\Logging");
Action.Trace("Reg Key Exists = " + ret);

ret =
Query.RegistryValueString(eLOCAL_MACHINE,"Software\\Novell\\Logging","test");
Action.Trace("Reg Value Is = " + ret);
```

VBScript:

```
dim ret
ret = Query.RegistryKeyExists(eLOCAL_MACHINE,"Software\\Novell\\Logging")
Action.Trace("Reg Key Exists = " & ret)

ret =
Query.RegistryValueString(eLOCAL_MACHINE,"Software\\Novell\\Logging","test")
Action.Trace("Reg Value Is = " & ret)
```

LocationName, LocationUuid, MaxConnectionSpeed, OSServicePack, PolicyName, PolicyTime, PolicyUuid, LocationIsStamped, TriggerEvent, TriggerEventData1

JScript:

```
var ret;
ret = Query.LocationName;
Action.Trace("Location Name = " + ret);
ret = Query.LocationUuid;
Action.Trace("Location Uuid = " + ret);
ret = Query.MaxConnectionSpeed;
Action.Trace("MaxConnectionSpeed = " + ret);
ret = Query.OSServicePack;
Action.Trace("OSServicePack = " + ret);
ret = Query.PolicyName;
```

```
Action.Trace("PolicyName = " + ret);
ret = Query.PolicyTime;
Action.Trace("PolicyTime = " + ret);
ret = Query.PolicyUuid;
Action.Trace("PolicyUuid = " + ret);
ret = Query.LocationIsStamped;
Action.Trace("LocationIsStamped = " + ret);
ret = Query.TriggerEvent;
Action.Trace("TriggerEvent = " + ret);
ret = Query.TriggerEventParameter;
Action.Trace("TriggerEventParameter = " + ret);
```

VBScript:

```
dim ret
ret = Query.LocationName
Action.Trace("Location Name = " & ret)
ret = Query.LocationUuid
Action.Trace("Location Uuid = " & ret)
ret = Query.MaxConnectionSpeed
Action.Trace("MaxConnectionSpeed = " & CLng(ret))
ret = Query.OSServicePack
Action.Trace("OSServicePack = " & ret)
ret = Query.PolicyName
Action.Trace("PolicyName = " & ret)
ret = Query.PolicyTime
Action.Trace("PolicyTime = " & ret)
ret = Query.PolicyUuid
Action.Trace("PolicyUuid = " & ret)
ret = Query.LocationIsStamped
Action.Trace("LocationIsStamped = " & ret)
ret = Query.TriggerEvent
Action.Trace("TriggerEvent = " & ret)
ret = Query.TriggerEventParameter
Action.Trace("TriggerEventParameter = " & ret)
```

RemovableMediaState, CDMediaState, HDCState, WiFiDisabledState, WiFiDisabledWhenWiredState, AdHocDisabledState, AdapterBridgeDisabledState, MinimumWiFiSecurityState, DialupDisabledState

JScript:

```
var ret;

Action.Trace("Reset Policy Change");
ret = Action.RemovableMediaState(-1, ePolicyChange);
Action.Trace("RemovableMediaState = " + ret);
ret = Action.CDMediaState(-1, ePolicyChange);
Action.Trace("CDMediaState = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eIrDA, ePolicyChange);
Action.Trace("\nHDCState(eApplyGlobalSetting, eIrDA) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, e1394, ePolicyChange);
Action.Trace("HDCState(eApplyGlobalSetting, e1394) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eBlueTooth, ePolicyChange);
Action.Trace("HDCState(eApplyGlobalSetting, eBlueTooth) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eSerialPort, ePolicyChange);
Action.Trace("HDCState(eApplyGlobalSetting, eSerialPort) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eParrallelPort, ePolicyChange);
```

```
Action.Trace("HDCState(eApplyGlobalSetting, eParrallelPort) = " + ret);
   ret = Action.WiFiDisabledState(eApplyGlobalSetting, ePolicyChange);
Action.Trace("\n WiFiDisabledState = " + ret);
ret = Action.WiFiDisabledWhenWiredState(eApplyGlobalSetting, ePolicyChange);
Action.Trace("WiFiDisabledWhenWiredState = " + ret);
ret = Action.AdHocDisabledState(eApplyGlobalSetting, ePolicyChange);
Action.Trace("AdHocDisabledState = " + ret);
ret = Action.AdapterBridgeDisabledState(eApplyGlobalSetting, ePolicyChange);
Action.Trace("AdapterBridgeDisabledState = " + ret);
ret = Action.MinimumWiFiSecurityState(eGlobalSetting, ePolicyChange);
Action.Trace("MinimumWiFiSecurityState = " + ret);
ret = Action.WiredDisabledState(eGlobalSetting, ePolicyChange);
Action.Trace("WiredDisabledState = " + ret);
ret = Action.DialupDisabledState(eGlobalSetting, ePolicyChange);
Action.Trace("DialupDisabledState = " + ret);
Action.Trace("Reset Location Change state");
ret = Action.RemovableMediaState(-1, eLocationChange);
Action.Trace("RemovableMediaState = " + ret);
ret = Action.CDMediaState(-1, eLocationChange);
Action.Trace("CDMediaState = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eIrDA, eLocationChange);
Action.Trace("\n HDCState(eApplyGlobalSetting, eIrDA) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, e1394, eLocationChange);
Action.Trace("HDCState(eApplyGlobalSetting, e1394) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eBlueTooth, eLocationChange);
Action.Trace("HDCState(eApplyGlobalSetting, eBlueTooth) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eSerialPort, eLocationChange);
Action.Trace("HDCState(eApplyGlobalSetting, eSerialPort) = " + ret);
ret = Action.HDCState(eApplyGlobalSetting, eParrallelPort, eLocationChange);
Action.Trace("HDCState(eApplyGlobalSetting, eParrallelPort) = " + ret);
   ret = Action.WiFiDisabledState(eApplyGlobalSetting, eLocationChange);
Action.Trace("\n WiFiDisabledState = " + ret);
ret = Action.WiFiDisabledWhenWiredState(eApplyGlobalSetting, eLocationChange);
Action.Trace("WiFiDisabledWhenWiredState = " + ret);
ret = Action.AdHocDisabledState(eApplyGlobalSetting, eLocationChange);
Action.Trace("AdHocDisabledState = " + ret);
ret = Action.AdapterBridgeDisabledState(eApplyGlobalSetting, eLocationChange);
Action.Trace("AdapterBridgeDisabledState = " + ret);
ret = Action.MinimumWiFiSecurityState(eGlobalSetting, eLocationChange);
Action.Trace("MinimumWiFiSecurityState = " + ret);
ret = Action.WiredDisabledState(eGlobalSetting, eLocationChange);
Action.Trace("WiredDisabledState = " + ret);
ret = Action.DialupDisabledState(eGlobalSetting, eLocationChange);
Action.Trace("DialupDisabledState = " + ret);
```

VBScript:

```
dim ret;
Action.Trace("Reset Policy Change")
ret = Action.RemovableMediaState(-1, ePolicyChange)
Action.Trace("RemovableMediaState = " & ret)
ret = Action.CDMediaState(-1, ePolicyChange)
Action.Trace("CDMediaState = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eIrDA, ePolicyChange)
Action.Trace("\n HDCState(eApplyGlobalSetting, eIrDA) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, e1394, ePolicyChange)
Action.Trace("HDCState(eApplyGlobalSetting, e1394) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eBlueTooth, ePolicyChange)
Action.Trace("HDCState(eApplyGlobalSetting, eBlueTooth) = " & ret)
```

```
ret = Action.HDCState(eApplyGlobalSetting, eSerialPort, ePolicyChange)
Action.Trace("HDCState(eApplyGlobalSetting, eSerialPort) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eParrallelPort, ePolicyChange)
Action.Trace("HDCState(eApplyGlobalSetting, eParrallelPort) = " & ret)
   ret = Action.WiFiDisabledState(eApplyGlobalSetting, ePolicyChange)
Action.Trace("\nWiFiDisabledState = " & ret)
ret = Action.WiFiDisabledWhenWiredState(eApplyGlobalSetting, ePolicyChange)
Action.Trace("WiFiDisabledWhenWiredState = " & ret)
ret = Action.AdHocDisabledState(eApplyGlobalSetting, ePolicyChange)
Action.Trace("AdHocDisabledState = " & ret)
ret = Action.AdapterBridgeDisabledState(eApplyGlobalSetting, ePolicyChange)
Action.Trace("AdapterBridgeDisabledState = " & ret)
ret = Action.MinimumWiFiSecurityState(eGlobalSetting, ePolicyChange)
Action.Trace("MinimumWiFiSecurityState = " & ret)
ret = Action.WiredDisabledState(eGlobalSetting, ePolicyChange)
Action.Trace("WiredDisabledState = " & ret)
ret = Action.DialupDisabledState(eGlobalSetting, ePolicyChange)
Action.Trace("DialupDisabledState = " & ret)
Action.Trace("Reset Location Change state")
ret = Action.RemovableMediaState(-1, eLocationChange)
Action.Trace("RemovableMediaState = " & ret)
ret = Action.CDMediaState(-1, eLocationChange)
Action.Trace("CDMediaState = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eIrDA, eLocationChange)
Action.Trace("\nHDCState(eApplyGlobalSetting, eIrDA) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, e1394, eLocationChange)
Action.Trace("HDCState(eApplyGlobalSetting, e1394) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eBlueTooth, eLocationChange)
Action.Trace("HDCState(eApplyGlobalSetting, eBlueTooth) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eSerialPort, eLocationChange)
Action.Trace("HDCState(eApplyGlobalSetting, eSerialPort) = " & ret)
ret = Action.HDCState(eApplyGlobalSetting, eParrallelPort, eLocationChange)
Action.Trace("HDCState(eApplyGlobalSetting, eParrallelPort) = " & ret)
   ret = Action.WiFiDisabledState(eApplyGlobalSetting, eLocationChange)
Action.Trace("\nWiFiDisabledState = " & ret)
ret = Action.WiFiDisabledWhenWiredState(eApplyGlobalSetting, eLocationChange)
Action.Trace("WiFiDisabledWhenWiredState = " & ret)
ret = Action.AdHocDisabledState(eApplyGlobalSetting, eLocationChange)
Action.Trace("AdHocDisabledState = " & ret)
ret = Action.AdapterBridgeDisabledState(eApplyGlobalSetting, eLocationChange)
Action.Trace("AdapterBridgeDisabledState = " & ret)
ret = Action.MinimumWiFiSecurityState(eGlobalSetting, eLocationChange)
Action.Trace("MinimumWiFiSecurityState = " & ret)
ret = Action.WiredDisabledState(eGlobalSetting, eLocationChange)
Action.Trace("WiredDisabledState = " & ret)
ret = Action.DialupDisabledState(eGlobalSetting, eLocationChange)
Action.Trace("DialupDisabledState = " & ret)
```

RemovableMediaState, CDMediaState, HDCState, IsWiFiDisabled, IsWiFiDisabledWhenWired, IsAdHocDisabled, IsAdapterBridgeDisabled, MinimumWiFiSecurityState, IsWiredDisabled, IsDialupDisabled

JScript:

```
var ret;
   Action.Trace("Status");
   ret = Query.RemovableMediaState();
   Action.Trace(   "RemovableMediaState = " + ret);
   ret = Query.CDMediaState();
   Action.Trace( "CDMediaState = " + ret);
   ret = Query.HDCState(eIrDA);
   Action.Trace("\n HDCState(eIrDA) = " + ret);
   ret = Query.HDCState(e1394);
   Action.Trace( "HDCState(e1394) = " + ret);
   ret = Query.HDCState(eBlueTooth);
   Action.Trace( "HDCState(eBlueTooth) = " + ret);
   ret = Query.HDCState(eSerialPort);
   Action.Trace( "HDCState(eSerialPort) = " + ret);
   ret = Query.HDCState(eParrallelPort);
   Action.Trace( "HDCState(eParrallelPort) = " + ret);
      ret = Query.IsWiFiDisabled();
   Action.Trace("\n IsWiFiDisabled = " + ret);
   ret = Query.IsWiFiDisabledWhenWired();
   Action.Trace( "IsWiFiDisabledWhenWired = " + ret);
   ret = Query.IsAdHocDisabled();
   Action.Trace( "IsAdHocDisabled = " + ret);
   ret = Query.IsAdapterBridgeDisabled();
   Action.Trace( "IsAdapterBridgeDisabled = " + ret);
   ret = Query.MinimumWiFiSecurityState();
   Action.Trace( "MinimumWiFiSecurityState = " + ret);
   ret = Query.IsWiredDisabled();
   Action.Trace( "IsWiredDisabled = " + ret);
   ret = Query.IsDialupDisabled();
   Action.Trace( "IsDialupDisabled = " + ret);
```

VBScript:

```
dim ret;
   Action.Trace("Status")
   ret = Query.RemovableMediaState()
   Action.Trace( "RemovableMediaState = " & ret)
   ret = Query.CDMediaState()
   Action.Trace( "CDMediaState = " & ret)
   ret = Query.HDCState(eIrDA)
   Action.Trace("\n HDCState(eIrDA) = " & ret)
   ret = Query.HDCState(e1394)
   Action.Trace( "HDCState(e1394) = " & ret)
   ret = Query.HDCState(eBlueTooth)
   Action.Trace( "HDCState(eBlueTooth) = " & ret)
   ret = Query.HDCState(eSerialPort)
   Action.Trace( "HDCState(eSerialPort) = " & ret)
   ret = Query.HDCState(eParrallelPort)
   Action.Trace( "HDCState(eParrallelPort) = " & ret)
      ret = Query.IsWiFiDisabled()
   Action.Trace("\n IsWiFiDisabled = " & ret)
   ret = Query.IsWiFiDisabledWhenWired()
   Action.Trace( "IsWiFiDisabledWhenWired = " & ret)
   ret = Query.IsAdHocDisabled()
   Action.Trace( "IsAdHocDisabled = " & ret)
   ret = Query.IsAdapterBridgeDisabled()
   Action.Trace( "IsAdapterBridgeDisabled = " & ret)
   ret = Query.MinimumWiFiSecurityState()
   Action.Trace( "MinimumWiFiSecurityState = " & ret)
   ret = Query.IsWiredDisabled()
   Action.Trace( "IsWiredDisabled = " & ret)
   ret = Query.IsDialupDisabled()
   Action.Trace( "IsDialupDisabled = " & ret)
```

Storage Namespace

There are two kinds of storage in the Endpoint Security Client storage space. Persistent storage remains between sessions of the client, while transient storage exists only for the duration of the client. Transient values can be accessed in each rule script invocation. Also, persistent storage can only store and retrieve string values, while transient storage store and retrieve those values that a VARIANT can hold.

NOTE: Each script variable stored in the "secure store" is preceded by a "rule id" (one for each script). Variables that need to be shared between scripts MUST have a forward slash BEFORE the variable name in EACH "persist" function accessing them to make that variable global, or accessible, to each script:

Example - "global" variable between scripts: "boolWarnedOnPreviousLoop"

```
Storage.PersistValueExists("/boolWarnedOnPreviousLoop");
```

SetNameValue, NameValueExists, GetNameValue

JScript:

```
var ret;
Storage.SetNameValue("testval",5);
ret = Storage.NameValueExists("testval");
Action.Trace("NameValueExists = " + ret);
ret = Storage.GetNameValue("testval");
Action.Trace("GetNameValue = " + ret);
```

VBScript:

```
dim ret
Storage.SetNameValue "testval",5
ret = Storage.NameValueExists("testval")
Action.Trace("NameValueExists = " & ret)
ret = Storage.GetNameValue("testval")
Action.Trace("GetNameValue = " & ret)
```

SetPersistString, PersistValueExists, GetPersistString

JScript:

```
var ret;
Storage.SetPersistString("teststr","pstring");
ret = Storage.PersistValueExists("teststr");
Action.Trace("PersistValueExists = " + ret);
ret = Storage.GetPersistString("teststr");
Action.Trace("GetPersistString = " + ret);
```

VBScript:

```
dim ret
Storage.SetPersistString "teststr", "pstring"
ret = Storage.PersistValueExists("teststr")
Action.Trace("PersistValueExists = " & ret)
ret = Storage.GetPersistString("teststr")
Action.Trace("GetPersistString = " & ret)
```

RuleState

JScript:

```
Storage.RuleState = true;
var ret = Storage.RuleState;
Action.Trace("RuleState = " + ret);
```

VBScript:

```
dim ret
Storage.RuleState = true
ret = Storage.RuleState
Action.Trace("RuleState = " & ret)
```

RetrySeconds

JScript:

```
var ret;
Storage.RetrySeconds = 30;
ret = Storage.RetrySeconds;
Action.Trace("RetrySeconds = " + ret);
```

VBScript:

```
dim ret
Storage.RetrySeconds = 30
ret = Storage.RetrySeconds
Action.Trace("RetrySeconds = " & ret)
```

Interfaces

These interfaces are returned by one of the methods of the namespaces described in section 3 or by one of the methods or properties of the following interfaces.

IClientAdapter Interface

This interface returns information about an adapter.

GetNetworkEnvironment

JScript:

```
var adplist;
var adplength;
var adp;
var env;
var ret;

adplist = Query.GetAdapters();
```

```
adplength = adplist.Length;

Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
  adp = adplist.Item(0);
  env = adp.GetNetworkEnvironment();
  ret = env.DHCPCount;
  Action.Trace("DHCPCount = " + ret);
  ret = env.DNSCount;
  Action.Trace("DNSCount = " + ret);
  ret = env.GatewayCount;
  Action.Trace("GatewayCount = " + ret);
  ret = env.WINSCount;
  Action.Trace("WINSCount = " + ret);
}
```

VBScript:

```
dim adplist
dim adplength
dim adp
dim env
dim ret

set adplist = Query.GetAdapters()
adplength = adplist.Length

Action.Trace("adplength = " & CInt(adplength))

if(CInt(adplength) > 0) then
  set adp = adplist.Item(0)
  set env = adp.GetNetworkEnvironment()
  ret = env.DHCPCount
  Action.Trace("DHCPCount = " & ret)
  ret = env.DNSCount
  Action.Trace("DNSCount = " & ret)
  ret = env.GatewayCount
  Action.Trace("GatewayCount = " & ret)
  ret = env.WINSCount
  Action.Trace("WINSCount = " & ret)
end if
```

DeviceID

See Query Namespace - GetAdapters

Enabled

See Query Namespace - GetAdapters

IP

See Query Namespace - GetAdapters

MAC

See Query Namespace - GetAdapters

MaxSpeed

See Query Namespace - GetAdapters

Name

See Query Namespace - GetAdapters

SubNetMask

See Query Namespace - GetAdapters

Type

See Query Namespace - GetAdapters

IClientEnvData Interface

This interface returns environment data about a Server or Wireless Access Point.

IP

See Query Namespace - GetLocationMatchData

MAC

See Query Namespace - GetLocationMatchData

SSIP

See Query Namespace - GetLocationMatchData

Type

See Query Namespace - GetLocationMatchData

IClientNetEnv Interface

This interface provides Network Environment Information.

GetDHCPItem

JScript:

```
var adplist;
var adplength;
var adp;
var env;
var ret;
var item;
```

```
adplist = Query.GetAdapters();
adplength = adplist.Length;

Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
  adp = adplist.Item(0);
  env = adp.GetNetworkEnvironment();

  ret = env.DHCPCount;
  Action.Trace("DHCPCount = " + ret);
  if(ret > 0)
  {
    item = env.GetDHCPItem(0);
    ret = item.IP;
    Action.Trace("IP = " + ret);
  }
}
```

VBScript:

```
dim adplist
dim adplength
dim adp
dim env
dim ret
dim item

set adplist = Query.GetAdapters()
adplength = adplist.Length

Action.Trace("adplength = " & CInt(adplength))

if(CInt(adplength) > 0) then
  set adp = adplist.Item(0)
  set env = adp.GetNetworkEnvironment()

  ret = env.DHCPCount
  Action.Trace("DHCPCount = " & ret)
  if(ret > 0) then
    set item = env.GetDHCPItem(0)
    ret = item.IP
    Action.Trace("IP = " & ret)
  end if
end if
```

GetDNSItem

JScript:

```
var adplist;
var adplength;
var adp;
var env;
var ret;
var item;

adplist = Query.GetAdapters();
```

```
adplength = adplist.Length;

Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
  adp = adplist.Item(0);
  env = adp.GetNetworkEnvironment();

  ret = env.DNSCount;
  Action.Trace("DNSCount = " + ret);
  if(ret > 0)
  {
    item = env.GetDNSItem(0);
    ret = item.IP;
    Action.Trace("IP = " + ret);
  }
}
```

VBScript:

```
dim adplist
dim adplength
dim adp
dim env
dim ret
dim item

set adplist = Query.GetAdapters()
adplength = adplist.Length

Action.Trace("adplength = " & CInt(adplength))

if(CInt(adplength) > 0) then
  set adp = adplist.Item(0)
  set env = adp.GetNetworkEnvironment()

  ret = env.DNSCount
  Action.Trace("DNSCount = " & ret)
  if(ret > 0) then
    set item = env.GetDNSItem(0)
    ret = item.IP
    Action.Trace("IP = " & ret)
  end if
end if
```

GetGatewayItem

JScript:

```
var adplist;
var adplength;
var adp;
var env;
var ret;
var item;

adplist = Query.GetAdapters();
adplength = adplist.Length;
```

```
Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
  adp = adplist.Item(0);
  env = adp.GetNetworkEnvironment();

  ret = env.GatewayCount;
  Action.Trace("GatewayCount = " + ret);
  if(ret > 0)
  {
    item = env.GetGatewayItem(0);
    ret = item.IP;
    Action.Trace("IP = " + ret);
  }
}
```

VBScript:

```
dim adplist
dim adplength
dim adp
dim env
dim ret
dim item

set adplist = Query.GetAdapters()
adplength = adplist.Length

Action.Trace("adplength = " & CInt(adplength))

if(CInt(adplength) > 0) then
  set adp = adplist.Item(0)
  set env = adp.GetNetworkEnvironment()

  ret = env.GatewayCount
  Action.Trace("GatewayCount = " & ret)
  if(ret > 0) then
    set item = env.GetGatewayItem(0)
    ret = item.IP
    Action.Trace("IP = " & ret)
  end if
end if
```

GetWINSItem

JScript:

```
var adplist;
var adplength;
var adp;
var env;
var ret;
var item;

adplist = Query.GetAdapters();
adplength = adplist.Length;
```

```
Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
  adp = adplist.Item(0);
  env = adp.GetNetworkEnvironment();

  ret = env.WINSCount;
  Action.Trace("WINSCount = " + ret);
  if(ret > 0)
  {
    item = env.GetWINSItem(0);
    ret = item.IP;
    Action.Trace("IP = " + ret);
  }
}
```

VBScript:

```
dim adplist
dim adplength
dim adp
dim env
dim ret
dim item

set adplist = Query.GetAdapters()
adplength = adplist.Length

Action.Trace("adplength = " & CInt(adplength))

if(CInt(adplength) > 0) then
  set adp = adplist.Item(0)
  set env = adp.GetNetworkEnvironment()

  ret = env.WINSCount
  Action.Trace("WINSCount = " & ret)
  if(ret > 0) then
    set item = env.GetWINSItem(0)
    ret = item.IP
    Action.Trace("IP = " & ret)
  end if
end if
```

GetWirelessAPItem, WirelessAPCount

JScript:

```
var adplist;
var adplength;
var adp;
var env;
var apitem;
var adptype;
var adpname;
var apcount;
var i;

adplist = Query.GetAdapters();
```

```
adplength = adplist.Length;
Action.Trace("adplength = " + adplength);

if(adplength > 0)
{
   for(i=0;i < adplength;i++)
  {
    adp = adplist.Item(i);
    adptype = adp.Type;
    if(adptype == eWIRELESS)
    {
      Action.Trace("Wireless index = " + i);
      adpname = adp.Name;
      Action.Trace("adp = " + adpname);

      env = adp.GetNetworkEnvironment();
      apcount = env.WirelessAPCount;
      Action.Trace("WirelessAPCount = " + apcount);
      if(apcount > 0)
      {
        apitem = env.GetWirelessAPItem(0);
        Action.Trace("apitem.SSID = " + apitem.SSID);
      }
    }
  }
}
```

VBScript:

```
dim adplist
dim adplength
dim adp
dim env
dim apitem
dim adptype
dim adpname
dim apcount
dim i

set adplist = Query.GetAdapters()
adplength = adplist.Length
Action.Trace("adplength = " & CInt(adplength))

if(CInt(adplength) > 0) then
  For i = 0 To (CInt(adplength) - 1)
    set adp = adplist.Item(i)
    adptype = adp.Type
    if(adptype = eWIRELESS) then
      Action.Trace("Wireless index = " & i)
      adpname = adp.Name
      Action.Trace("adp = " & adpname)

      set env = adp.GetNetworkEnvironment()
      apcount = env.WirelessAPCount
      Action.Trace("WirelessAPCount = " & apcount)
      if(apcount > 0) then
        set apitem = env.GetWirelessAPItem(0)
        Action.Trace("apitem.SSID = " & apitem.SSID)
      end if
    end if
  Next
end if
```

DHCPCount

See ICLIENTADAPTER Interface - GetNetworkEnvironment

DNSCount

See ICLIENTADAPTER Interface - GetNetworkEnvironment

GatewayCount

See ICLIENTADAPTER Interface - GetNetworkEnvironment

WINSCount

See ICLIENTADAPTER Interface - GetNetworkEnvironment

WirelessAPCount

See ICLIENTADAPTER Interface - GetNetworkEnvironment

IClientWAP Interface

This interface provides information about a Wireless Access Point.

AvgRssi

See IClientNetEnv Interface - GetWirelessAPItem

MAC

See IClientNetEnv Interface - GetWirelessAPItem

MaxRssi

See IClientNetEnv Interface - GetWirelessAPItem

MinRssi

See IClientNetEnv Interface - GetWirelessAPItem

Rssi

See IClientNetEnv Interface - GetWirelessAPItem

SSID

See IClientNetEnv Interface - GetWirelessAPItem

IClientAdapterList Interface

This interface is a list of adapters in the network environment.

Item & Length

See Query Namespace - GetAdapters

6.4 Importing and Exporting Policies

The following sections contain more information:

- Section 6.4.1, "Importing Policies," on page 169
- Section 6.4.2, "Exporting a Policy," on page 169
- Section 6.4.3, "Exporting Policies to Unmanaged Users," on page 169

6.4.1 Importing Policies

A policy can be imported from any file location on the available network.

1. In the Management Console, click *File* > *Import Policy*.

   If you are currently editing or drafting a policy, the editor closes the policy (prompting you to save it) before opening the Import window.
2. Browse to specify the file location and specify the filename in the provided field.

After the policy is imported, it can be further edited or immediately published.

6.4.2 Exporting a Policy

Policies can be exported from the Management Console and distributed via e-mail or through a network share. This can be used to distribute enterprise-level policies in environments where multiple Management Services and Policy Editors are deployed.

To export a security policy:

1. In the Mangement Console, click *File* > *Export*.
2. Enter a destination and give the policy a name with an extension of .sen (for example, `C:\Desktop\salespolicy.sen`) If in doubt, click the browse button to browse to a location.
3. Click *Export*.

Two files are exported. The first file is the policy (*.sen file). The second file is the `setup.sen` file, which is required to decrypt the policy at import.

Exported policies must be imported into a Management Console before they can be published to managed users.

6.4.3 Exporting Policies to Unmanaged Users

If unmanaged Endpoint Security Clients have been deployed within the enterprise, a Stand-Alone Management Console must be installed to create policies.

To distribute unmanaged polices:

1 Locate and copy the Management Console `setup.sen` file to a separate folder.

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

2 Create a policy in the Management Console. For more information, see Section 6.2, "Creating Security Policies," on page 79.

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` in order for the Endpoint Security Client to accept them.

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

The `setup.sen` file needs to be copied to the unmanaged Endpoint Security Clients only once with the first policy. Afterwards, only new policies must be distributed.

6.5 Sample Scripts

The following sections contain sample script that you can use and modify:

- Section 6.5.1, "Create Registry Shortcut (VB Script)," on page 170
- Section 6.5.2, "Allow Only One Connection Type (JScript)," on page 172
- Section 6.5.3, "Stamp Once Script," on page 173

6.5.1 Create Registry Shortcut (VB Script)

'This script is to run at startup of the Endpoint Security Client.

'The script creates a desktop and program files shortcut that is linked to a VBScript file that the script also creates. The VBScript is located in the Endpoint Security Client installation folder. It sets a registry entry to TRUE. A second script, included in the policy, reads this registry entry. If the entry is TRUE, it launches the dialog box that allows the user to control wireless adapters.This script also disables wireless adapters at startup. Per customer request, Modems are also disabled because the 3G wireless card instantiate as modems.

```
'*************** Global Varialbles
set WshShell = CreateObject ("WScript.Shell")
Dim strStartMenu
strStartMenu = WshShell.SpecialFolders("AllUsersPrograms")
Dim strDesktop
strDesktop = WshShell.SpecialFolders("AllUsersDesktop")

'*************** Main Loop
DisableWirelessAdapters()
CreateStartMenuFolder()
CreateStartMenuProgramFilesShortcut()
CreateDesktopAllUsersShortcut()
CreateVbsFileToWriteRegEntry()
```

```
'*************** Functions to do each action
Function DisableWirelessAdapters()
   Dim ret
   'NOTE:    1 means this action can be undone on a location change if
the policy allows
   '      0 means this action can be undone on a policy update if the policy
allows
   ret = Action.WiFiDisabledState(eDisableAccess, 1)
   Action.Trace("Disallow Wi-Fi = " & ret)
   'Again, per the customer request, Modems will be disabled to deal with 3G
wireless cards that act as modems in the network stack
   ret = Action.DialupDisabledState ( eDisableAccess , 1 )
   Action.Trace("Disallow Modem = " & ret)
End Function

Function CreateStartMenuProgramFilesShortcut()
   'create the Start Menu folder and then create the shortcut
   set oShellLinkStartMenu = WshShell.CreateShortcut (strStartMenu &
"\Novell\Enable Wireless Adapter Control.lnk")
  oShellLinkStartMenu.TargetPath = "C:\Program Files\Novell ZENworks\Endpoint
Security Client\wareg.vbs"
   oShellLinkStartMenu.WindowStyle = 1
   oShellLinkStartMenu.Hotkey = "CTRL+SHIFT+W"
   oShellLinkStartMenu.IconLocation = "C:\Program Files\Novell
ZENworks\Endpoint Security Client\STEngine.exe, 0"
   oShellLinkStartMenu.Description = "Launch Novell Wireless Adapter Control
Dialog Box"
   oShellLinkStartMenu.WorkingDirectory = "C:\Program Files\Novell
ZENworks\Endpoint Security Client"
   oShellLinkStartMenu.Save
End Function

Function CreateDesktopAllUsersShortcut()
   'create the desktop folder shortcut
   set oShellLinkDesktop = WshShell.CreateShortcut (strDesktop & "\Enable
Wireless Adapter Control.lnk")
   oShellLinkDesktop.TargetPath = "C:\Program Files\Novell ZENworks\Endpoint
Security Client\wareg.vbs"
   oShellLinkDesktop.WindowStyle = 1
   oShellLinkDesktop.Hotkey = "CTRL+SHIFT+W"
   oShellLinkDesktop.IconLocation = "C:\Program
Files\Novell ZENworks\Endpoint Security Client\STEngine.exe, 0"
   oShellLinkDesktop.Description = "Launch Novell Wireless Adapter
Control Dialog Box"
   oShellLinkDesktop.WorkingDirectory = "C:\Program
Files\Novell ZENworks\Endpoint Security Client"
   oShellLinkDesktop.Save
End Function

Function CreateVbsFileToWriteRegEntry()
   'First build the VBScript file to write the registry key
   Dim pathToTempVbsFile
   pathToTempVbsFile = "C:\Program Files\Novell ZENworks\Endpoint Security
Client\wareg.vbs"
   Dim ofileSysObj, fileHandle
   set ofileSysObj = CreateObject ( "Scripting.FileSystemObject" )
   set fileHandle = ofileSysObj.CreateTextFile ( pathToTempVbsFile , true )
   fileHandle.WriteLine "Dim WshShell"
   fileHandle.WriteLine "Set WshShell = CreateObject(""WScript.Shell"")"
   fileHandle.WriteLine "WshShell.RegWrite ""HKLM\SOFTWARE\Novell\MSC\STUWA"",
""true"", ""REG_SZ"""
   fileHandle.Close
   Action.Trace ("Wrote the VBScript file to: " + pathToTempVbsFile )
End Function

Function CreateStartMenuFolder
     Dim fso, f, startMenuSenforceFolder
    startMenuSenforceFolder = strStartMenu & "\Novell"
   Set fso = CreateObject("Scripting.FileSystemObject")
   If (fso.FolderExists(startMenuSenforceFolder)) Then
      Action.Trace(startMenuSenforceFolder & " Already exists, so NOT creating
it.")
   Else
      Action.Trace("Creating folder: " & startMenuSenforceFolder)
         Set f = fso.CreateFolder(startMenuSenforceFolder)
         CreateFolderDemo = f.Path
   End If
End Function
```

6.5.2 Allow Only One Connection Type (JScript)

```
// Disable Wired and Wireless if Dialup is connection
// Disable Modem and Wired if Wireless is connected
// Disable Modem and Wireless if Wired is connected
// Reenable all hardware (based off policy settings) if there are NO active
network connections

//NOTE:  The order for checking sets the precedence for allowed connections
//    As coded below, Wired is first, then Wireless, then Modem.  So if
//    you have both a wired and modem connection when this script is
//    launched, then the modem will be disabled (i.e. the wired is preferred)

var CurLoc = Query.LocationName;
Action.Trace("CurLoc is: " + CurLoc);
if (CurLoc ==  "Desired Location")
{//only run this script if the user is in the desired location.  This MUST
MATCH the exact name of the location in the policy
}

var Wired = Query.IsAdapterTypeConnected( eWIRED );
Action.Trace("Connect Status of Wired is: " + Wired);
var Wireless = Query.IsAdapterTypeConnected( eWIRELESS );
Action.Trace("Connect Status of Wireless is: " + Wireless );
var Dialup = Query.IsAdapterTypeConnected( eDIALUPCONN );
Action.Trace("Connect Status of Dialup is: " + Dialup );

var wiredDisabled = Query.IsWiredDisabled();
Action.Trace("Query on WiredDisabled is: " + wiredDisabled );

var wifiDisabled = Query.IsWiFiDisabled();
Action.Trace("Query on WifiDisabled is: " + wifiDisabled );

var dialupDisabled = Query.IsDialupDisabled();
Action.Trace("Query on DialupDisabled is: " + dialupDisabled );

//check if there is a wired connection
if (Wired)
```

```
{
   Action.Trace ("Wired Connection Only!");
   Action.DialupDisabledState ( eDisableAccess , 0 );
   Action.WiFiDisabledState ( eDisableAccess , 0) ;
   //alternative call
   //Action.EnableAdapterType (false, eDIALUPCONN );
   //Action.EnableAdapterType (false, eWIRELESS );
}
else
{
   Action.Trace("NO Wired connection found.");
}

//check if there is a wireless connection
if (Wireless)
{
   Action.Trace ("Wireless Connection Only!");
   Action.WiredDisabledState ( eDisableAccess , 0);
   Action.DialupDisabledState ( eDisableAccess , 0);
   //alternative call
   //Action.EnableAdapterType (false, eDIALUPCONN );
   //Action.EnableAdapterType (false, eWIRED );
}
else
{
   Action.Trace("NO Wireless connection found.");
}

//check if there is a modem connection
if (Dialup)
{
   Action.Trace ("Dialup Connection Only!");
   Action.WiredDisabledState ( eDisableAccess , 0);
   Action.WiFiDisabledState ( eDisableAccess , 0);
   //alternative call
   //Action.EnableAdapterType (false, eWIRED );
   //Action.EnableAdapterType (false, eWIRELESS );
}
else
{
   Action.Trace("NO Dialup connection found.");
}
if (( !Wired ) && ( !Wireless ) && ( !Dialup ))
{//Apply Global settings so you don't override policy settings
   Action.Trace("NO connections so, enable all");
   Action.DialupDisabledState ( eApplyGlobalSetting , 1);
   Action.WiredDisabledState ( eApplyGlobalSetting , 1);
   Action.WiFiDisabledState ( eApplyGlobalSetting , 1);
}
```

6.5.3 Stamp Once Script

The Stamp Once script enforces a single network environment save at a designated location. When users enter the desired network environment, they should be instructed to switch to the location assigned below and then perform a network environment save . After this environment has been saved, the Endpoint Security Client does not permit additional network environments to be saved at that location.

NOTE: This script works best when used for an environment that will likely not change its network parameters (for example, an end-user's home network or a satellite office). If network identifiers change (IP or MAC addresses) the Endpoint Security Client might not be able to recognize the location and remains in the default Unknown location.

To initiate the Stamp Once Script:

1. Under Locations, create or select the location that will use the Stamp Once functionality.
2. Under User Permissions, uncheck Save Network Environment.
3. Associate the Stamp Once scripting rule to this policy.
4. Set the triggering event to Location Change: Activate when switching to. Select the configured location from the previous steps.
5. Open the location_locked variable and select the same location.

Managing the Endpoint Security Client 3.5

7

Novell® ZENworks® Endpoint Security Management uses the Endpoint Security Client, installed on each endpoint device, to enforce complete security. There are two versions: Endpoint Security Client 3.5 and Endpoint Security Client 4.0.

The Endpoint Security Client 3.5 is installed on Windows XP and Windows 2000 enterprise computers. The Novell ZENworks Endpoint Security Client 4.0 is a client release to support Microsoft Windows Vista with Support Pack 1 running in 32-bit mode. Both Endpoint Security Clients use the ZENworks Endpoint Security Management 3.5 Server and Management Console.

This section discusses managing Endpoint Security Client 3.5. For managing Endpoint Security Client 4.0, see Chapter 8, "Managing the Endpoint Security Client 4.0," on page 191.

The following sections contain more information:

- Section 7.1, "Understanding the Endpoint Security Client," on page 175
- Section 7.2, "Installing and Uninstalling the ZENworks Security Agent," on page 176
- Section 7.3, "Understanding Client Self Defense," on page 177
- Section 7.4, "Upgrading the Endpoint Security Client 3.5," on page 178
- Section 7.5, "Running the Endpoint Security Client 3.5," on page 178
- Section 7.6, "Using the Endpoint Security Client Diagnostics Tools," on page 180

7.1 Understanding the Endpoint Security Client

The Endpoint Security Client protects client data by determining in real-time the network location of the endpoint. Based on that location, the Endpoint Security Client does the following:

- Implements policy-based filtering of all incoming and outgoing traffic.
- Implements policy-based control over hardware use (such as WLAN adaptor connections to access points, removable media, and network adapters).
- Validates anti-virus software status.
- Collects security-centric statistics and event traps, and passes that information to centralized servers for collation and analysis.
- Launches nominated applications in policy-defined situations (for example, if a policy is set so that in a certain location, a VPN program must be used to access the network, that program is launched).

If the network environment is not recognized, the Endpoint Security Client sets the location to a default Unknown location, and applies the Unknown security policy. Security policies are completely configurable by the Endpoint Security Management administrator. For Endpoint Security Client operating instructions, see the *ZENworks Endpoint Security Client 3.5 User Guide* or the *ZENworks Endpoint Security Client 4.0 User Guide*.

All Endpoint Security Client security functionality is determined by the security policy.

7.2 Installing and Uninstalling the ZENworks Security Agent

The following sections contain more information:

- Section 7.2.1, "Installing the Endpoint Security Client 3.5," on page 176
- Section 7.2.2, "Uninstalling the Endpoint Security Client 3.5," on page 176

7.2.1 Installing the Endpoint Security Client 3.5

Before you begin:

- Verify that all security patches for Microsoft and anti-virus software are installed and up-to-date. The Endpoint Security Client 3.5 software can be installed on Windows XP running Support Pack 1, 2, or 3 and on Windows 2000 running Support Pack 4.

  NOTE: Some features, like encryption, are not supported on Windows 2000.

- Novell recommends that antivirus/spyware software that is interacting with valid registry functions be shut down during the installation of the Endpoint Security Client 3.5.
- The Managed Endpoint Security Client requires SSL communication to the ZENworks Endpoint Security Management Service component. If you selected "self signed certificates" during the Management Service or the Single Server installation, the endpoint running the Security Client must have the certificate installed in the proper context (preferably in the local computer context).

  To do this automatically, place the `ESM-MS.cer` file in the folder along with the Endpoint Security Client installer's `Setup.exe` file. Optionally, you can copy the entire `ESM Setup Files` folder from the Management Service installation (or Single Server installation) into the folder with the Endpoint Security Client installer `Setup.exe` (ensure that the `ESM-MS.cert` is in the `ESM Setup Files` folder and the folder is named `ESM Setup Files`). This automatically installs the certificate onto the machine (for example, for all users). This process can also be done with the Novell license`.dat` file.

For installation instructions, see "Endpoint Security Client 3.5 Installation" in the *ZENworks Endpoint Security Management Installation Guide*.

7.2.2 Uninstalling the Endpoint Security Client 3.5

The following sections provide instructions for performing an attended uninstall and an unattended (silent) uninstall:

- "Preparing a Machine for Client Uninstallation" on page 177
- "Performing an Attended Uninstall" on page 177
- "Performing an Unattended (Silent) Uninstall" on page 177

Preparing a Machine for Client Uninstallation

Before uninstalling the Security Client on a machine, you should do the following:

- Distribute a simple policy to the machine. Policies that globally disable Wi-Fi functionality also disable any communication hardware, and storage devices can leave the hardware disabled following uninstallation, requiring you to manually re-enable each device.
- Eject the wireless card prior to uninstallation, switch off the Wi-Fi radio, and close all software with a network connection (for example, VPN or FTP software).

Performing an Attended Uninstall

To uninstall the Security Client, do one of the following:

- Click *Start* > *Programs* > *Novell* > *ZENworks Security Client* > *Uninstall ZENworks Security Client*.
- Run the `setup.exe` program using the following command syntax:

  ```
  setup.exe /V"STUNINSTALL=1"
  ```
- Run Windows Installer using the following command syntax:

  ```
  msiexec.exe /x {C1773AE3-3A47-48EB-9338-7FF2CDC73E67} STUNINSTALL=1
  ```

To specify the uninstall password when using `setup.exe` or `msiexec.exe`, use the `STUIP=`*`password`* option. For example:

```
setup.exe /V"STUNINSTALL=1 STUIP=removeZESM"
```

Performing an Unattended (Silent) Uninstall

To perform a silent uninstall the Security Client, do one of the following:

- Run the `setup.exe` program using the following command syntax:

  ```
  setup.exe /s /x /V"/qn STUNINSTALL=1"
  ```
- Run Windows Installer using the following command syntax:

  ```
  msiexec.exe /x /qn {C1773AE3-3A47-48EB-9338-7FF2CDC73E67} STUNINSTALL=1
  ```

If the Security Client requires an uninstall password, use the `STUIP=`*`password`* option. For example:

```
setup.exe /s /x /V"/qn STUNINSTALL=1 STUIP=removeZESM"
```

7.3 Understanding Client Self Defense

The Endpoint Security Client is protected from being intentionally or unintentionally uninstalled, shut down, disabled, or tampered with in any way that would expose sensitive data to unauthorized users. Each measure protects the client against a specific vulnerability:

- Normal uninstall is not allowed without an installation password (if implemented, see the *ZENworks Endpoint Security Management Installation Guide*), or an uninstall MSI is pushed down by the administrator.
- Windows Task Manager requests to terminate `STEngine.exe` and `STUser.exe` processes are disallowed.

- Service Pause/Stop and client uninstall is controlled by password, defined in the policy,
- Critical files and registry entries are protected and monitored. If an invalid change is made to any of the keys or values, the registry is immediately changed back to valid values.
- NDIS filter driver binding protection is enabled. If the NDIS driver is not bound to each adapter, `STEngine` rebinds the NDIS filter driver.

7.4 Upgrading the Endpoint Security Client 3.5

You can upgrade the Endpoint Security Client by doing one of the following:

- By utilizing the Endpoint Security Client Update option. For more information, see "ZSC Update" on page 94.
- By running the new install executable (the default name is `setup.exe`) with the `STUPGRADE=1` switch activated, on each client machine.
- By running an MSI uninstall of the current Endpoint Security Client and running a new installation (MSI cannot perform upgrades).

7.4.1 Setting the Upgrade Switch

1. Open the new installation package for the Endpoint Security Client, then right-click `setup.exe`.
2. Click *Create Shortcut*.
3. Right-click the shortcut, then click *Properties*.
4. At the end of the Target field, after the quotes, press the Spacebar once to insert a space, then type `/V"STUPGRADE=1"`

   Example: `"C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /V"STUPGRADE=1"`.
5. Click *OK*.
6. Double-click the shortcut to launch the upgrade installer.

7.5 Running the Endpoint Security Client 3.5

The Endpoint Security Client 3.5 runs automatically at system startup. For user operation of the Endpoint Security Client, see the *ZENworks Endpoint Security Client 3.5 User Guide*.

You can distribute the guide to all users to help them better understand the operation of their new security software.

The following sections contain more information:

- Section 7.5.1, "Multiple User Support," on page 179
- Section 7.5.2, "Machine-Based Policies (Active Directory Only)," on page 179
- Section 7.5.3, "Distributing Unmanaged Policies," on page 179

7.5.1 Multiple User Support

For machines that have multiple users logging on to them, each user account has its own, separate Novell environment. Users can have separate policies and saved network environments. Each account needs to log in to the Management Service separately to receive its credential in order to download its published policy.

If a user can't log in or refuses to do so, that user gets the initial policy that was included at Endpoint Security Client installation. This helps discourage a user from creating a different account to avoid policy restrictions.

Multiple user support is set at the time you install the client, and can only be changed through an MSI property (POLICYTYPE 0=user or 1=computer) when you upgrade the client (see "MSI Installation" the *ZENworks Endpoint Security Management Installation Guide* for details).

Because only one policy can be enforced at a time, the Microsoft Fast User Switching (FUS) is not supported. The Endpoint Security Client turns off FUS at installation.

For an unmanaged client, the first policy that is pushed to one of the users is applied to all users until the other users enforce their policies.

The users on a single computer must all be managed or unmanaged. If they are managed, all the users must use the same Management and Policy Distribution Service.

7.5.2 Machine-Based Policies (Active Directory Only)

The option for using machine-based rather than user-based policies is set at Endpoint Security Client installation (see the *ZENworks Endpoint Security Management Installation Guide* for details). When this option is selected, the machine is assigned the policy from the Management Service, and the policy is applied to all users who log on to that machine. Users who have a policy assigned to them on another machine do not have that policy accompany them when they log on to a machine with a machine-based policy. Instead, the machine-based policy is enforced.

NOTE: The machine must be a member of the Policy Distribution Service's domain for the first policy sent down. Occasionally, Microsoft does not immediately generate the SID, which can prevent the Endpoint Security Client on that machine from receiving its credential from the Management Service. When this occurs, reboot the machine when the Endpoint Security Client installation is finished to receive the credentials.

When you switch an Endpoint Security Client from accepting user-based policies to accepting machine-based policies, the client continues to enforce and use the last policy downloaded by the current user, until credentials are provided. If multiple users exist on the machine, the machine uses only the policy assigned to the currently logged-in user. If a new user logs in, and the SID is unavailable, the machine uses the default policy included at installation, until the SID is available. After the SID is available for the endpoint, all users have the machine-based policy applied.

7.5.3 Distributing Unmanaged Policies

To distribute polices to unmanaged Endpoint Security Clients:

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 the `\Program Files\Novell\ESM Management Console\` directory.

2. Create a policy in the Management Console. For more information, see Chapter 6, “Creating and Distributing Security Policies,” on page 75.
3. Use the Export command (see Section 6.4.3, “Exporting Policies to Unmanaged Users,” on page 169) to export the policy to the same folder containing the `setup.sen` file. All policies distributed must be named `policy.sen` for an unmanaged Endpoint Security Client to accept them.
4. Distribute the `policy.sen` and `setup.sen` files. These files must be copied to the `\Program Files\Novell ZENworks\Endpoint Security Client\` directory for all unmanaged clients.

The `setup.sen` file must be copied to the unmanaged Endpoint Security Clients only once, along with the first policy. Afterwards, only new policies need to be distributed.

7.6 Using the Endpoint Security Client Diagnostics Tools

The Endpoint Security Client features several diagnostics tools that can create a customized diagnostics package that can then be delivered to Novell Support to help resolve any issues. Optionally, logging and reporting can be activated to provide full details regarding endpoint usage. Administrators can also view the current policy, add rule scripting, and check the Endpoint Security Client driver status.

The following sections contain more information:

- Section 7.6.1, “Creating a Diagnostics Package,” on page 180
- Section 7.6.2, “Administrator Views,” on page 182
- Section 7.6.3, “Logging,” on page 186
- Section 7.6.4, “Reporting,” on page 187

7.6.1 Creating a Diagnostics Package

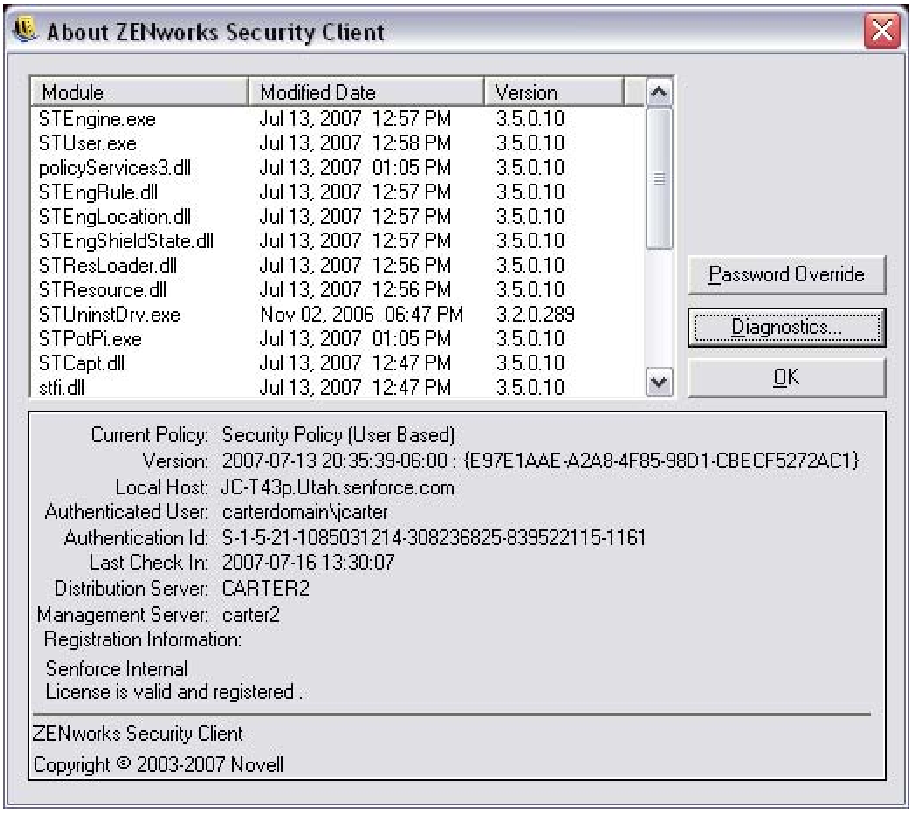
If problems occur because of the Endpoint Security Client’s presence on the endpoint, administrators can provide detailed diagnostics information packages to Novell Support. This information is vital in resolution of any issues. The diagnostics package is defined by the following items:

- **Bindings:** Captures the current driver bindings for the endpoint.
- **Client Status:** Captures the current client status (displayed on the About window) as well as other internal status.
- **Driver Status:** Captures the current status of all drivers on the endpoint (displayed in the Driver Status window).
- **Group Policy Object:** Captures the current GPO for the user/endpoint as designated by your directory service (for example., Active Directory).
- **Log Files:** Captures the designated logs (see Section 7.6.3, “Logging,” on page 186).
- **Policy:** Captures the current policy running on the Endpoint Security Client (see “View Policy” on page 183).
- **Network Environments:** Captures the current and detected network environments.

- **Registry Settings:** Captures the current registry settings.
- **Reports:** Captures any reports in the `temp` directory (see Section 7.6.4, “Reporting,” on page 187).
- **System Event Logs:** Captures the current System Event logs.
- **System Information:** Captures all system information.

To create a diagnostics package:

1 Right-click the *Endpoint Security Client* icon, then click *About*.



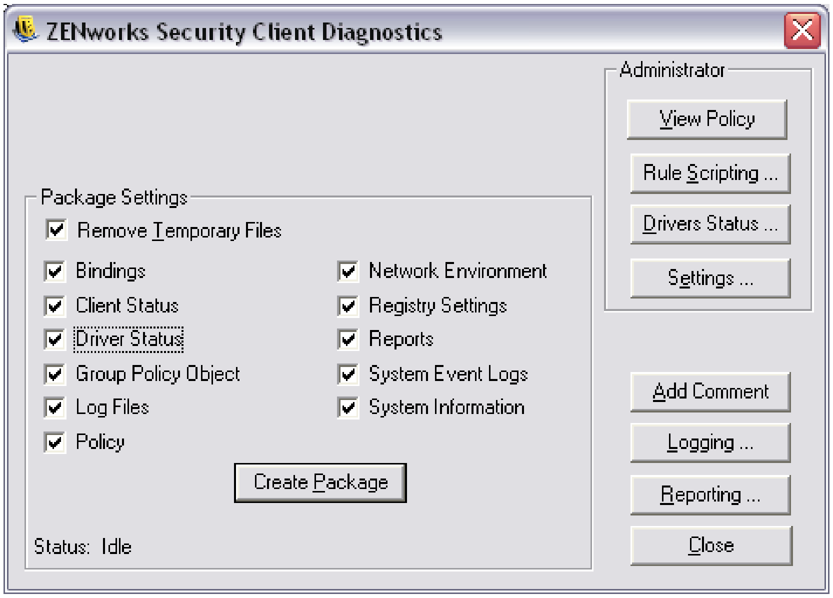
About ZENworks Security Client

Module	Modified Date	Version
STEngine.exe	Jul 13, 2007 12:57 PM	3.5.0.10
STUser.exe	Jul 13, 2007 12:58 PM	3.5.0.10
policyServices3.dll	Jul 13, 2007 01:05 PM	3.5.0.10
STEngRule.dll	Jul 13, 2007 12:57 PM	3.5.0.10
STEngLocation.dll	Jul 13, 2007 12:57 PM	3.5.0.10
STEngShieldState.dll	Jul 13, 2007 12:57 PM	3.5.0.10
STResLoader.dll	Jul 13, 2007 12:56 PM	3.5.0.10
STResource.dll	Jul 13, 2007 12:56 PM	3.5.0.10
STUninstDrv.exe	Nov 02, 2006 06:47 PM	3.2.0.289
STPotPi.exe	Jul 13, 2007 01:05 PM	3.5.0.10
STCapt.dll	Jul 13, 2007 12:47 PM	3.5.0.10
stfi.dll	Jul 13, 2007 12:47 PM	3.5.0.10

Current Policy: Security Policy (User Based)
Version: 2007-07-13 20:35:39-06:00 : {E97E1AAE-A2A8-4F85-98D1-CBECF5272AC1}
Local Host: JC-T43p.Utah.senforce.com
Authenticated User: carterdomain\jcarter
Authentication Id: S-1-5-21-1085031214-308236825-839522115-1161
Last Check In: 2007-07-16 13:30:07
Distribution Server: CARTER2
Management Server: carter2
Registration Information:
Senforce Internal
License is valid and registered .

ZENworks Security Client
Copyright © 2003-2007 Novell

2 Click *Diagnostics*.



ZENworks Security Client Diagnostics

Package Settings

☑ Remove Temporary Files

☑ Bindings
☑ Client Status
☑ Driver Status
☑ Group Policy Object
☑ Log Files
☑ Policy
☑ Network Environment
☑ Registry Settings
☑ Reports
☑ System Event Logs
☑ System Information

Status: Idle

3 Select the items to be included in the package (all are selected by default).

4 Click *Create Package* to generate the package.

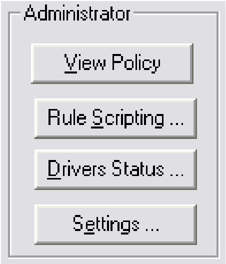
The generated package (`ESSDiagnostics_YYYYMMDD_HHMMSS.zip.enc`) is available on the desktop. This encrypted zip file can now be sent to Technical Support.

The Remove Temporary Files setting, which is only available when a password override is active in the policy, can be deselected to keep each package component type in a temporary directory. This setting should be deselected only when a Novell Professional Services representative is present on-site and wants to check individual logs. Otherwise, the files that are generated are not necessary and take up disk space over time.

7.6.2 Administrator Views

The Administrator views for the diagnostic tools, such the *Remove Temporary Files* check box, display only when a password override is present in the policy. The *View Policy* button requires that either the password or a temporary password to be entered. After the password is entered, it does not need to be entered again, as long as the diagnostics window remains open.

Figure 7-1 *Administrator Views*



The following sections contain more information:

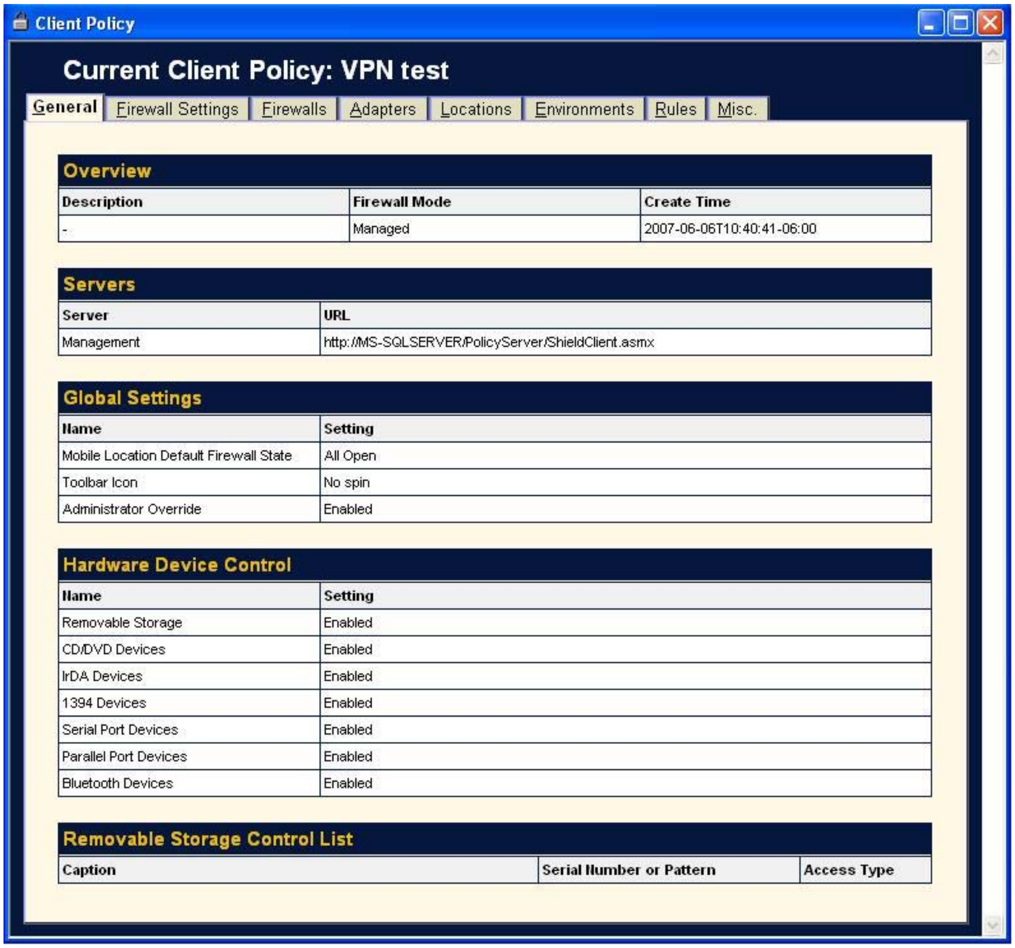
- "View Policy" on page 183

- "Rule Scripting" on page 184
- "Driver Status" on page 184
- "Settings" on page 185

View Policy

The *View Policy* button displays the current policy on the device. The display shows basic policy information and can be used to troubleshoot suspected policy issues.

Figure 7-2 *View Policy Window*



Client Policy

Current Client Policy: VPN test

Overview

Description	Firewall Mode	Create Time
-	Managed	2007-06-06T10:40:41-06:00

Servers

Server	URL
Management	http://MS-SQLSERVER/PolicyServer/ShieldClient.asmx

Global Settings

Name	Setting
Mobile Location Default Firewall State	All Open
Toolbar Icon	No spin
Administrator Override	Enabled

Hardware Device Control

Name	Setting
Removable Storage	Enabled
CD/DVD Devices	Enabled
IrDA Devices	Enabled
1394 Devices	Enabled
Serial Port Devices	Enabled
Parallel Port Devices	Enabled
Bluetooth Devices	Enabled

Removable Storage Control List

Caption	Serial Number or Pattern	Access Type

The policy display divides the policy components into the following tabs:

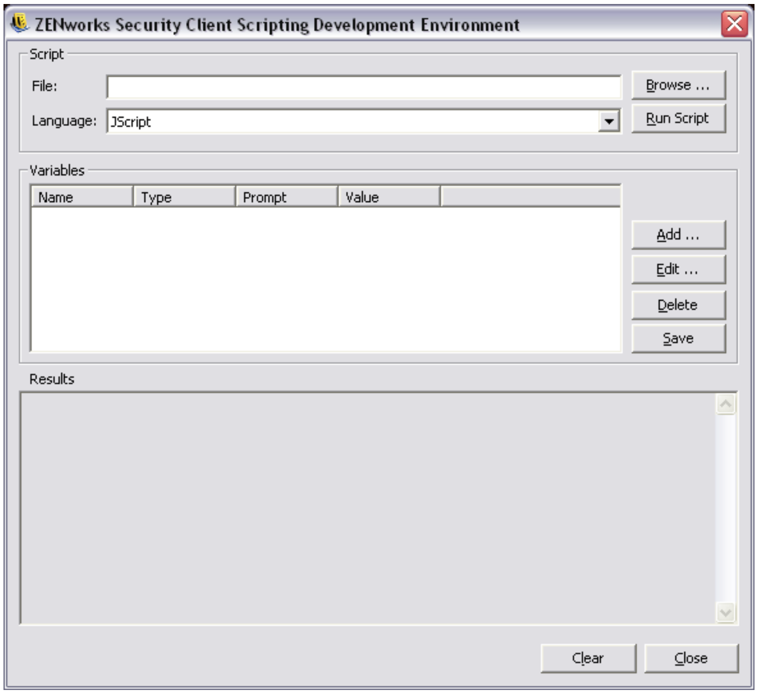
- **General:** Displays the global and default settings for the policy.
- **Firewall Settings:** Displays the Port, ACL, and Application groups available in this policy.
- **Firewalls:** Displays the firewalls and their individual settings.
- **Adapters:** Displays the permitted network adapters.
- **Locations:** Displays each location, and the settings for each.
- **Environments:** Displays the settings for defined network environments.
- **Rules:** Displays integrity and scripting rules in this policy.

- **Misc:** Displays assigned reporting, hyperlinks, and custom user messages for this policy.

Rule Scripting

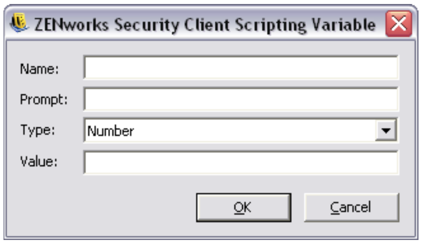
The *Rule Scripting* button allows the administrator to enter a specific script into the Endpoint Security Client that runs on this endpoint only. You can use the scripting window to browse for an available script (scripts must be either jscript or vbscript), or a script can be created by using this tool.

Figure 7-3 *Rule Scripting Window*



Variables are created by clicking *Add*, which displays a second window where the variable information can be entered.

Figure 7-4 *Scripting Variable Window*

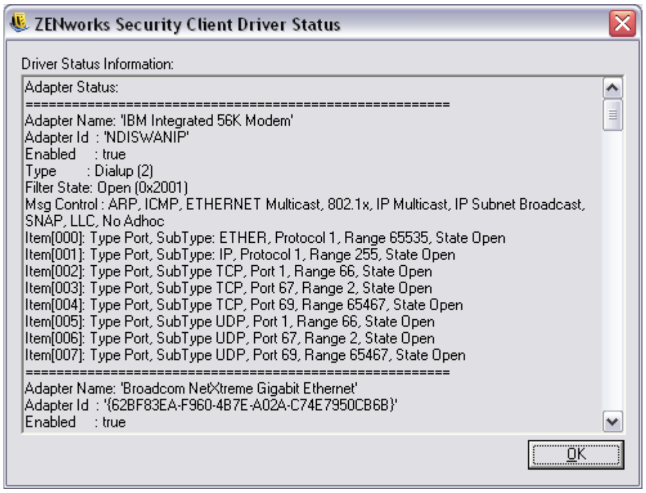


Editing a variable launches the same window, where you can edit as needed. *Delete* removes the variable. Click *Save* in the main scripting window after a variable is set.

Driver Status

The *Driver Status* button displays the current status of all drivers and affected components.

Figure 7-5 Client Driver Status Window



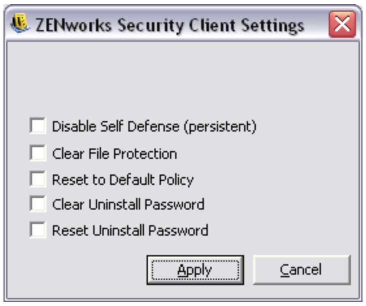
ZENworks Security Client Driver Status
Driver Status Information:
OK

```
Adapter Status:
======================================================
Adapter Name: 'IBM Integrated 56K Modem'
Adapter Id  : 'NDISWANIP'
Enabled     : true
Type        : Dialup (2)
Filter State: Open (0x2001)
Msg Control : ARP, ICMP, ETHERNET Multicast, 802.1x, IP Multicast, IP Subnet Broadcast,
SNAP, LLC, No Adhoc
Item[000]: Type Port, SubType: ETHER, Protocol 1, Range 65535, State Open
Item[001]: Type Port, SubType: IP, Protocol 1, Range 255, State Open
Item[002]: Type Port, SubType TCP, Port 1, Range 66, State Open
Item[003]: Type Port, SubType TCP, Port 67, Range 2, State Open
Item[004]: Type Port, SubType TCP, Port 69, Range 65467, State Open
Item[005]: Type Port, SubType UDP, Port 1, Range 66, State Open
Item[006]: Type Port, SubType UDP, Port 67, Range 2, State Open
Item[007]: Type Port, SubType UDP, Port 69, Range 65467, State Open
======================================================
Adapter Name: 'Broadcom NetXtreme Gigabit Ethernet'
Adapter Id  : '{62BF83EA-F960-4B7E-A02A-C74E7950CB6B}'
Enabled     : true
```

Settings

The *Settings* button lets administrators adjust the settings for the Endpoint Security Client without re-installing the software. Select the actions you want to perform, then click the *Apply* button:

Figure 7-6 Endpoint Security Client Settings Control



- □ Disable Self Defense (persistent)
- □ Clear File Protection
- □ Reset to Default Policy
- □ Clear Uninstall Password
- □ Reset Uninstall Password

The following sections contain more information:

- "Disable Self Defense" on page 185
- "Clear File Protection" on page 186
- "Reset to Default Policy" on page 186
- "Clear Uninstall Password" on page 186
- "Reset Uninstall Password" on page 186

Disable Self Defense

Disables all protections used to keep the client installed and active on the machine. Disabling should only be used when performing patch fixes to the Endpoint Security Client.

IMPORTANT: This must be deselected and applied again, or Client Self Defense remains off.

Clear File Protection

This will clear the hashes from the protected files. The current policies and licensing information will remain. Once the hashes are cleared, the file may be updated. This can only be performed while Client Self Defense is turned off.

Reset to Default Policy

Restores the original policy to permit check-in when the current policy is blocking access.

Clear Uninstall Password

This clears the password that is required for uninstalling the Endpoint Security Client. Once cleared, the Endpoint Security Client can be uninstalled without a password prompt. Use when the uninstall password is failing, or lost.

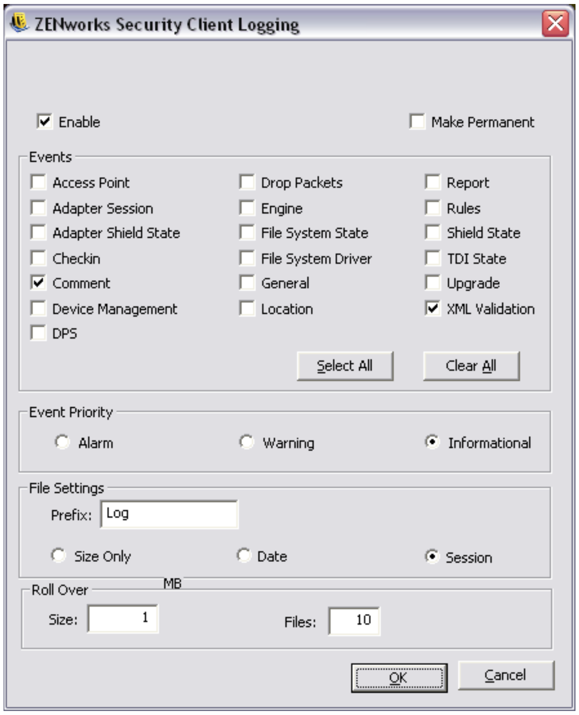
Reset Uninstall Password

Resets the password required to uninstall the Endpoint Security Client. The administrator will be prompted with a window to enter the new uninstall password.

7.6.3 Logging

Logging can be turned on for the Endpoint Security Client, permitting it to log specific system events. The default logs gathered by the Endpoint Security Client are XML Validation and Commenting. Additional logs can be selected from the checklist. When troubleshooting, it is recommended that logging be set according to the directions of Novell Technical Support and the circumstances that lead to the error be repeated.

Figure 7-7 *Logging Window*



ZENworks Security Client Logging

☑ Enable

□ Make Permanent

Events

□ Access Point
□ Adapter Session
□ Adapter Shield State
□ Checkin
☑ Comment
□ Device Management
□ DPS
□ Drop Packets
□ Engine
□ File System State
□ File System Driver
□ General
□ Location
□ Report
□ Rules
□ Shield State
□ TDI State
□ Upgrade
☑ XML Validation

Event Priority

○ Alarm ○ Warning ● Informational

File Settings

Prefix: Log

○ Size Only ○ Date ● Session

Roll Over

Size: 1 MB

Files: 10

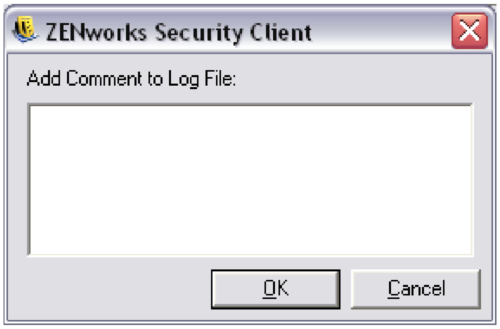
Additionally, the type of log created, file settings, and roll-over settings can be adjusted, based on your current needs.

To make the new logs record after the device's reboot, check the *Make Permanent* box, otherwise the Endpoint Security Client reverts to its default logs at the next reboot.

Add Comment

The option to add a comment to the logs is available on the diagnostics window. Click the *Add Comments* button to display the Add Comment window. Comments are included with the next batch of logs.

Figure 7-8 *Comment Window*

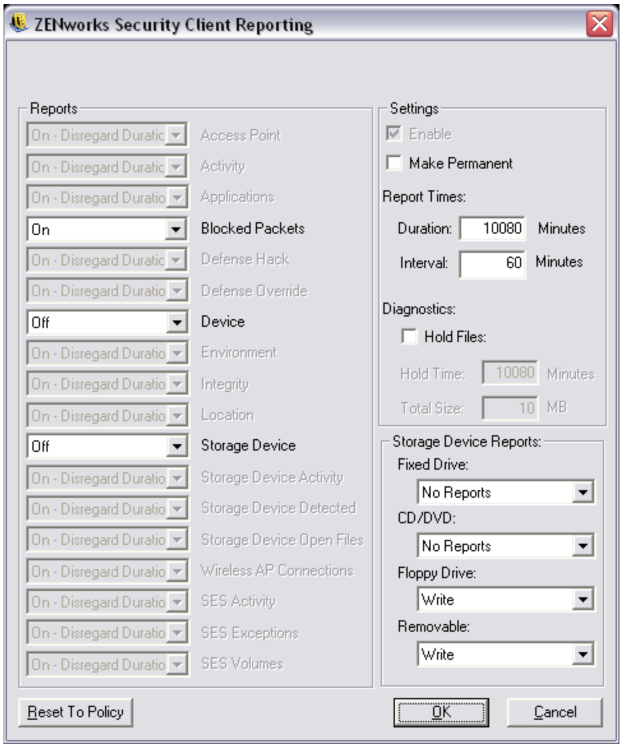


NOTE: If the *Comments* option in logging is unchecked, the *Add Comments* button does not display.

7.6.4 Reporting

Reporting allows the addition of reports for this endpoint. Reports can be added and increased in duration; however, reports cannot fall below what was already assigned by the policy (for example, specific reporting, if activated in the policy, cannot be turned off). See Section 6.2.4, "Compliance Reporting," on page 118 for descriptions of the report types.

Figure 7-9 *Reporting Overrides*



ZENworks Security Client Reporting

Reports

On - Disregard Duratic	Access Point
On - Disregard Duratic	Activity
On - Disregard Duratio	Applications
On	Blocked Packets
On - Disregard Duratic	Defense Hack
On - Disregard Duratio	Defense Override
Off	Device
On - Disregard Duratio	Environment
On - Disregard Duratio	Integrity
On - Disregard Duratio	Location
Off	Storage Device
On - Disregard Duratio	Storage Device Activity
On - Disregard Duratio	Storage Device Detected
On - Disregard Duratio	Storage Device Open Files
On - Disregard Duratio	Wireless AP Connections
On - Disregard Duratio	SES Activity
On - Disregard Duratio	SES Exceptions
On - Disregard Duratio	SES Volumes

Settings

☑ Enable

☐ Make Permanent

Report Times:

Duration: 10080 Minutes

Interval: 60 Minutes

Diagnostics:

☐ Hold Files:

Hold Time: 10080 Minutes

Total Size: 10 MB

Storage Device Reports:

Fixed Drive: No Reports

CD/DVD: No Reports

Floppy Drive: Write

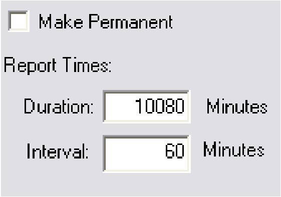
Removable: Write

The duration settings for each report include:

- **Off:** Data is not gathered.
- **On:** Data is gathered based on the set duration.
- **On - Disregard Duration:** The data is gathered indefinitely.

The duration and send interval can be set using the *Report Times* options on the right of the screen.

Figure 7-10 *Duration Settings, and Make Permanent*



☐ Make Permanent

Report Times:

Duration: 10080 Minutes

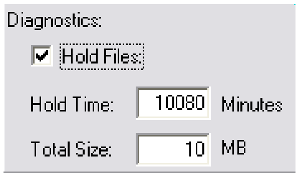
Interval: 60 Minutes

Check the *Make Permanent* box to continue uploading the new reports for just this end-user; otherwise, reporting reverts to the policy default at the device's next reboot.

Making Reports Available for a Diagnostics Package

To capture reports in the diagnostics package, check the *Hold Files* box in the Reporting window. This option causes reports to be retained in the `temp` directory for the time/space defined in the Reporting window. These reports can then be bundled in the diagnostics package.

Figure 7-11 *Hold Reports for Diagnostics*



Diagnostics:

☑ Hold Files:

Hold Time: 10080 Minutes

Total Size: 10 MB

Managing the Endpoint Security Client 4.0

8

Novell® ZENworks® Endpoint Security Management uses the Endpoint Security Client, installed on each endpoint device, to enforce complete security. There are two versions: Endpoint Security Client 3.5 and Endpoint Security Client 4.0.

The Endpoint Security Client 3.5 is installed on Windows XP and Windows 2000 enterprise computers. The Novell ZENworks Endpoint Security Client 4.0 is a client release to support Microsoft Windows Vista with Support Pack 1 running in 32-bit mode. Both Endpoint Security Clients use the ZENworks Endpoint Security Management 3.5 Server and Management Console.

This section discusses managing Endpoint Security Client 4.0. For managing Endpoint Security Client 3.5, see Chapter 7, “Managing the Endpoint Security Client 3.5,” on page 175.

The following sections contain more information:

- Section 8.1, “Understanding the Endpoint Security Client,” on page 191
- Section 8.2, “Installing and Uninstalling the ZENworks Security Agent,” on page 192
- Section 8.3, “Running the Endpoint Security Client 4.0,” on page 193
- Section 8.4, “Using the Endpoint Security Client Diagnostics Tools,” on page 195

8.1 Understanding the Endpoint Security Client

The Endpoint Security Client protects client data by determining, in real-time, the network location of the endpoint. Based on that location, the Endpoint Security Client does the following:

- Implements policy-based filtering for all incoming and outgoing network traffic.
- Implements policy-based control over hardware use (such as WLAN network adapters’ ad hoc connections).
- Launches nominated applications in policy-defined situations (for example, if a policy is set to require a VPN program in order to access the network, that program is launched).

If the network environment is not recognized, the Endpoint Security Client sets the location to a default Unknown location, and applies the Unknown security policy. Security policies are completely configurable by the Endpoint Security Management Administrator. For Endpoint Security Client operating instructions, see the *ZENworks Endpoint Security Client 3.5 User Guide* and *ZENworks Endpoint Security Client 4.0 User Guide*.

All Endpoint Security Client security functionality is determined by the security policy.

8.2 Installing and Uninstalling the ZENworks Security Agent

The following sections contain more information:

- Section 8.2.1, "Installing the Endpoint Security Client 4.0," on page 192
- Section 8.2.2, "Uninstalling the Endpoint Security Client 4.0," on page 192

8.2.1 Installing the Endpoint Security Client 4.0

Before you begin:

- Verify that all security patches for Microsoft and anti-virus software are installed and up to date. The Endpoint Security Client 4.0 software can be installed on Windows Vista running Support Pack 1 running in 32-bit mode.
- Novell recommends that antivirus/spyware software that is interacting with valid registry functions be shut down during the installation of the Endpoint Security Client 4.0.
- The Managed Endpoint Security Client requires SSL communication to the ZENworks Endpoint Security Management Service component. If you selected self-signed certificates during the Management Service or the Single Server installation, the endpoint running the Security Client must have the certificate installed in the proper context (preferably in the local computer context).

  To do this automatically, place the `ESM-MS.cer` file in the folder along with the Endpoint Security Client installer's `Setup.exe` file. Optionally, you can copy the entire `ESM Setup Files` folder from the Management Service installation (or Single Server installation) into the folder with the Endpoint Security Client installer `Setup.exe` (ensure that the `ESM-MS.cert` is in the `ESM Setup Files` folder and the folder is named `ESM Setup Files`). This automatically installs the certificate onto the machine (for example, for all users). This process can also be done with the Novell license`.dat` file.

For installation instructions, see "Endpoint Security Client 3.5 Installation" in the *ZENworks Endpoint Security Management Installation Guide*.

8.2.2 Uninstalling the Endpoint Security Client 4.0

The following sections provide instructions for performing an attended uninstall and an unattended (silent) uninstall:

- "Preparing a Machine for Client Uninstallation" on page 193
- "Performing an Attended Uninstall" on page 193
- "Performing an Unattended (Silent) Uninstall" on page 193

Preparing a Machine for Client Uninstallation

Before uninstalling the Security Client on a machine, you should do the following:

- Distribute a simple policy to the machine. Policies that globally disable Wi-Fi functionality also disable any communication hardware, and storage devices can leave the hardware disabled following uninstallation, requiring you to manually re-enable each device.
- Eject the wireless card prior to uninstallation, switch off the Wi-Fi radio, and close all software with a network connection (for example, VPN or FTP software).

Performing an Attended Uninstall

To uninstall the Security Client, do one of the following:

- Click *Start* > *Programs* > *Novell* > *ZENworks Security Client* > *Uninstall ZENworks Security Client*.
- Run the `setup.exe` program using the following command syntax:

  ```
  setup.exe /V"STUNINSTALL=1"
  ```
- Run Windows Installer using the following command syntax:

  ```
  msiexec.exe /x {6208B443-6136-484A-AF4A-74BEA8A3840E} STUNINSTALL=1
  ```

To specify the uninstall password when using `setup.exe` or `msiexec.exe`, use the `STUIP=`*`password`* option. For example:

```
setup.exe /V"STUNINSTALL=1 STUIP=removeZESM"
```

Performing an Unattended (Silent) Uninstall

To perform a silent uninstall the Security Client, do one of the following:

- Run the `setup.exe` program using the following command syntax:

  ```
  setup.exe /s /x /V"/qn STUNINSTALL=1"
  ```
- Run Windows Installer using the following command syntax:

  ```
  msiexec.exe /x /qn {6208B443-6136-484A-AF4A-74BEA8A3840E} STUNINSTALL=1
  ```

If the Security Client requires an uninstall password, use the `STUIP=`*`password`* option. For example:

```
setup.exe /s /x /V"/qn STUNINSTALL=1 STUIP=removeZESM"
```

8.3 Running the Endpoint Security Client 4.0

The Endpoint Security Client 4.0 runs automatically at system startup. For user operation of the Endpoint Security Client, see the *ZENworks Endpoint Security Client 4.0 User Guide*.

You can distribute the guide to all users to help them better understand the operation of their new security software.

The following sections contain more information:

- Section 8.3.1, “Multiple User Support,” on page 194

- Section 8.3.2, “Machine-Based Policies (Active Directory Only),” on page 194
- Section 8.3.3, “Distributing Unmanaged Policies,” on page 195

8.3.1 Multiple User Support

For machines that have multiple users logging on to them, each user account has its own, separate Novell environment. Users can have separate policies and saved network environments. Each account needs to log in to the Management Service separately to receive its credential in order to download its published policy.

Where a user can’t log in or refuses to do so, that user gets the initial policy that was included at Endpoint Security Client installation. This helps discourage a user from creating a different account to avoid policy restrictions.

Multiple user support is set at the time you install the client, and can only be changed when you upgrade the client through an MSI property (POLICYTYPE 0=user or 1=computer; see “MSI Installation” the *ZENworks Endpoint Security Management Installation Guide* for details).

Because only one policy can be enforced at a time, the Microsoft Fast User Switching (FUS) is not supported. The Endpoint Security Client turns off FUS at installation.

For an unmanaged client, the first policy that is pushed to one of the users is applied to all users until the other users enforce their policies.

The users on a single computer must all be managed or unmanaged. If they are managed, all the users must use the same Management and Policy Distribution Service.

8.3.2 Machine-Based Policies (Active Directory Only)

The option for using machine-based rather than user-based policies is set at Endpoint Security Client installation (see the *ZENworks Endpoint Security Management Installation Guide* for details). When this operation is selected, the machine is assigned the policy from the Management Service, and the policy is applied to all users who log on to that machine. Users who have a policy assigned to them on another machine do not have that policy accompany them when they log on to a machine with a machine-based policy. Instead, the machine-based policy is enforced.

NOTE: The machine must be a member of the Policy Distribution Service's domain for the first policy that is downloaded. Occasionally, Microsoft does not immediately generate the SID, which can prevent the Endpoint Security Client on that machine from receiving its credential from the Management Service. When this occurs, reboot the machine following complete Endpoint Security Client installation to receive the credentials.

Machine-based policy support is set at the time you install the client, and can only be changed when you upgrade the client through an MSI property (POLICYTYPE 0=user or 1=computer; see “MSI Installation” the *ZENworks Endpoint Security Management Installation Guide* for details).

8.3.3 Distributing Unmanaged Policies

To distribute policies to unmanaged Endpoint Security Clients:

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 the `\Program Files\Novell\ESM Management Console\` directory.
2. Create a policy in the Management Console. For more information, see Chapter 6, "Creating and Distributing Security Policies," on page 75.
3. Use the Export command (see Section 6.4.3, "Exporting Policies to Unmanaged Users," on page 169) to export the policy to the same folder containing the `setup.sen` file. All policies distributed must be named `policy.sen` for an unmanaged Endpoint Security Client to accept them.
4. Distribute the `policy.sen` and `setup.sen` files. These files must be copied to the `\Program Files\Novell ZENworks\Endpoint Security Client\` directory for all unmanaged clients.

The `setup.sen` file must be copied to the unmanaged Endpoint Security Clients only once, with the first policy. Afterwards, only new policies need to be distributed.

8.4 Using the Endpoint Security Client Diagnostics Tools

The Endpoint Security Client features several diagnostics tools that can create a customized diagnostics package to be delivered to Novell Support to resolve any issues. Optionally, logging and reporting can be activated to provide full details regarding endpoint usage. Administrators can also view the current policy, add rule scripting, and check the Endpoint Security Client driver status.

The following sections contain more information:

- Section 8.4.1, "Creating a Diagnostics Package," on page 195
- Section 8.4.2, "Administrator Views," on page 197
- Section 8.4.3, "Module List," on page 200
- Section 8.4.4, "Logging," on page 201

8.4.1 Creating a Diagnostics Package

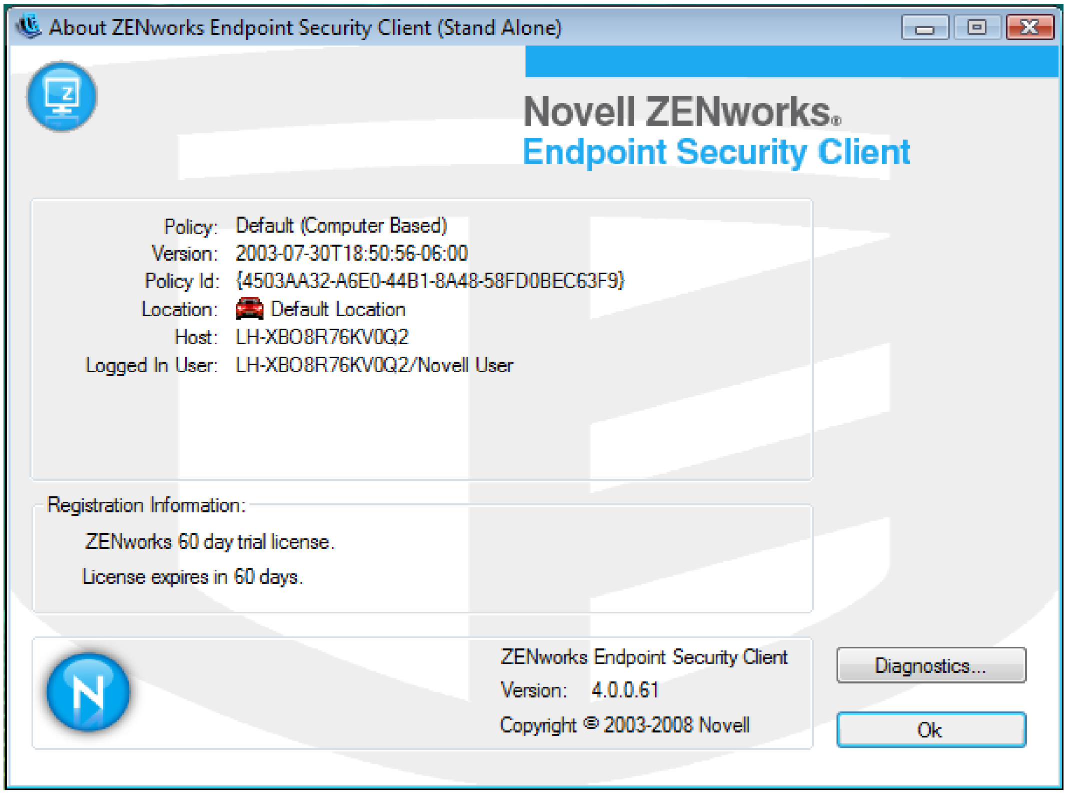
If problems occur because of the Endpoint Security Client's presence on the endpoint, administrators can provide detailed diagnostics information packages to Novell Support. This information is vital in resolution of any issues. The diagnostics package is defined by the following items:

- **Group Policy Object:** Captures the current GPO for the user/endpoint as designated by your directory service (for example, Active Directory).
- **Network Environments:** Captures the current and detected network environments.
- **Registry Settings:** Captures the current registry settings.
- **System Information:** Captures all system information.
- **System Event Logs:** Captures the current System Event logs.

- **Wireless Environment:** Captures the current and detected wireless environments.

To create a diagnostics package:

1 Right-click the Endpoint Security Client icon, then click *About*.



About ZENworks Endpoint Security Client (Stand Alone)

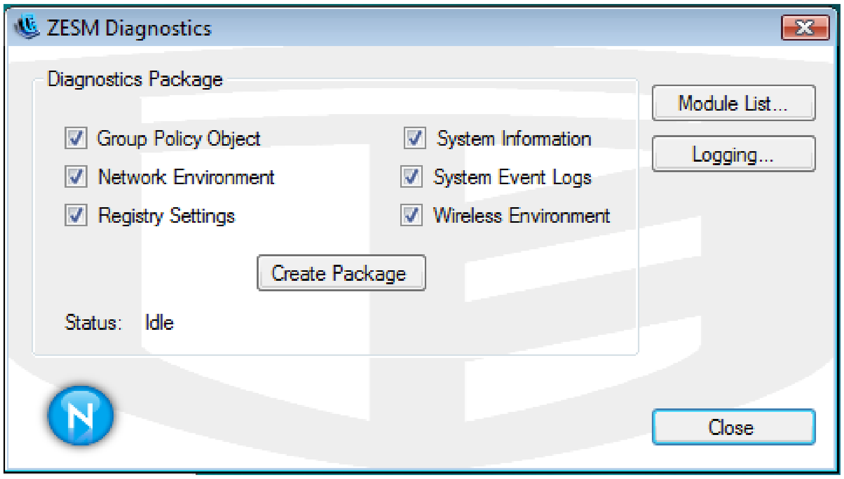
Novell ZENworks®
Endpoint Security Client

Policy: Default (Computer Based)
Version: 2003-07-30T18:50:56-06:00
Policy Id: {4503AA32-A6E0-44B1-8A48-58FD0BEC63F9}
Location: Default Location
Host: LH-XBO8R76KV0Q2
Logged In User: LH-XBO8R76KV0Q2/Novell User

Registration Information:
ZENworks 60 day trial license.
License expires in 60 days.

ZENworks Endpoint Security Client
Version: 4.0.0.61
Copyright © 2003-2008 Novell

2 Click *Diagnostics*.



ZESM Diagnostics

Diagnostics Package

☑ Group Policy Object
☑ Network Environment
☑ Registry Settings
☑ System Information
☑ System Event Logs
☑ Wireless Environment

Status: Idle

3 Select the items to be included in the package (all are selected by default).

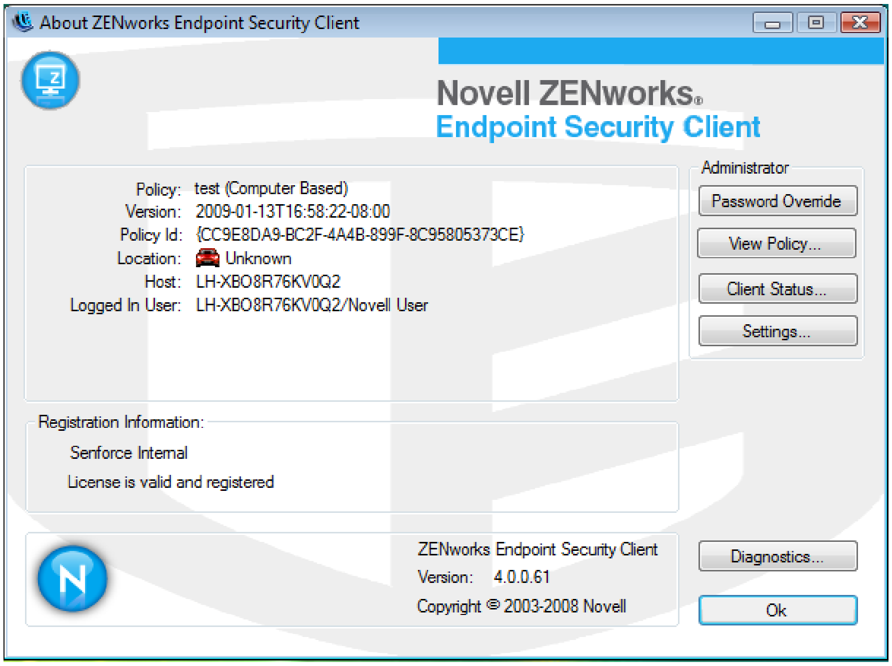
4 Click *Create Package* to generate the package.

The generated package (`ESSDiagnostics_YYYYMMDD_HHMMSS.zip.enc`) is available on the desktop. This encrypted zip file can now be sent to Support.

8.4.2 Administrator Views

The Administrator views display only when password override is present in the policy. The Administrator views are added to the right side of the Endpoint Security Client About window under the Administrator heading.

Figure 8-1 *Administrator Views*



Policy: test (Computer Based)
Version: 2009-01-13T16:58:22-08:00
Policy Id: {CC9E8DA9-BC2F-4A4B-899F-8C95805373CE}
Location: Unknown
Host: LH-XBO8R76KV0Q2
Logged In User: LH-XBO8R76KV0Q2/Novell User

Registration Information:
Senforce Internal
License is valid and registered

ZENworks Endpoint Security Client
Version: 4.0.0.61
Copyright © 2003-2008 Novell

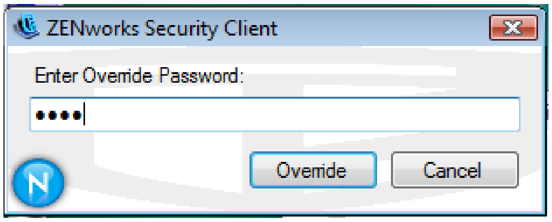
The following sections contain more information:

- "Password Override" on page 197
- "View Policy" on page 198
- "Client Status" on page 199
- "Settings" on page 199

Password Override

Use the *Password Override* button to temporarily override policy settings by loading an Allow-All policy. Type the password and click *Override*.

Figure 8-2 *Entering the Override Password*



Enter Override Password:
••••

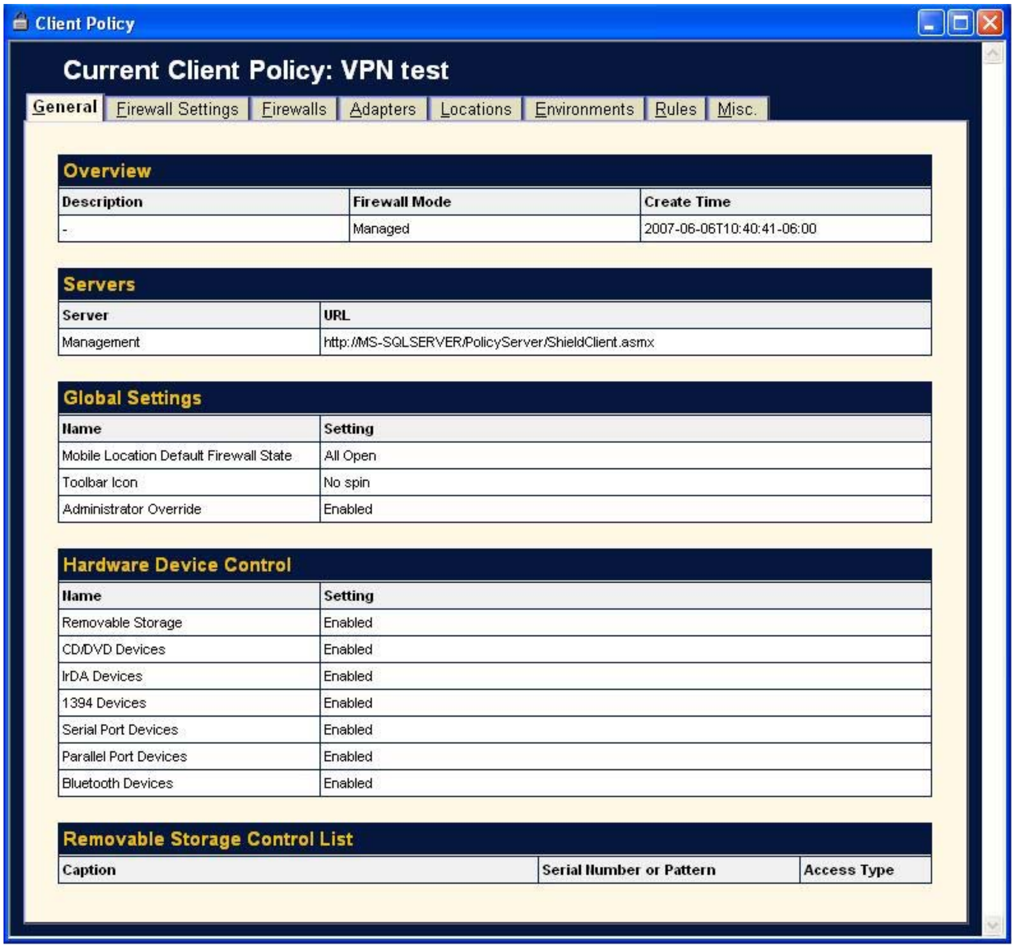
After the password is entered, the *Password Override* button changes into *Load Policy*. When you enter the password, you do not need to enter it again until you click the *Load Policy* button, which reverts back to the running user policy.

Password overrides can also be set up for a specified amount of time. When that time expires, the running user policy is again loaded and the *Password Override* button appears.

View Policy

The *View Policy* button displays the current policy on the device. The display shows basic policy information and can be used to troubleshoot suspected policy issues.

Figure 8-3 *View Policy Window*



Current Client Policy: VPN test

Overview

Description	Firewall Mode	Create Time
-	Managed	2007-06-06T10:40:41-06:00

Servers

Server	URL
Management	http://MS-SQLSERVER/PolicyServer/ShieldClient.asmx

Global Settings

Name	Setting
Mobile Location Default Firewall State	All Open
Toolbar Icon	No spin
Administrator Override	Enabled

Hardware Device Control

Name	Setting
Removable Storage	Enabled
CD/DVD Devices	Enabled
IrDA Devices	Enabled
1394 Devices	Enabled
Serial Port Devices	Enabled
Parallel Port Devices	Enabled
Bluetooth Devices	Enabled

Removable Storage Control List

Caption	Serial Number or Pattern	Access Type

The policy display divides the policy components into the following tabs:

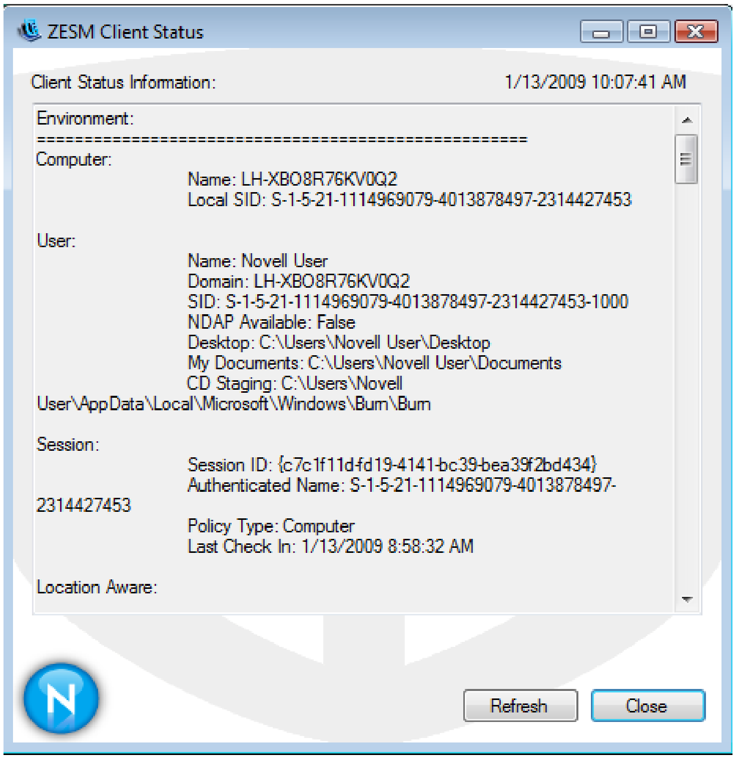
- **General:** Displays the global and default settings for the policy.
- **Firewall Settings:** Displays the Port, ACL, and Application groups available in this policy.
- **Firewalls:** Displays the firewalls and their individual settings.
- **Adapters:** Displays the permitted network adapters.
- **Locations:** Displays each location, and the settings for each.
- **Environments:** Displays the settings for defined network environments.

- **Rules:** Displays integrity and scripting rules in this policy.
- **Misc:** Displays assigned reporting, hyperlinks, and custom user messages for this policy.

Client Status

The *Client Status* button displays the current status of the client and affected components.

Figure 8-4 *ZESM Client Status Window*



```
Client Status Information:                              1/13/2009 10:07:41 AM

Environment:
====================================================
Computer:
                    Name: LH-XBO8R76KV0Q2
                    Local SID: S-1-5-21-1114969079-4013878497-2314427453

User:
                    Name: Novell User
                    Domain: LH-XBO8R76KV0Q2
                    SID: S-1-5-21-1114969079-4013878497-2314427453-1000
                    NDAP Available: False
                    Desktop: C:\Users\Novell User\Desktop
                    My Documents: C:\Users\Novell User\Documents
                    CD Staging: C:\Users\Novell
User\AppData\Local\Microsoft\Windows\Burn\Burn

Session:
                    Session ID: {c7c1f11d-fd19-4141-bc39-bea39f2bd434}
                    Authenticated Name: S-1-5-21-1114969079-4013878497-
2314427453
                    Policy Type: Computer
                    Last Check In: 1/13/2009 8:58:32 AM

Location Aware:
```

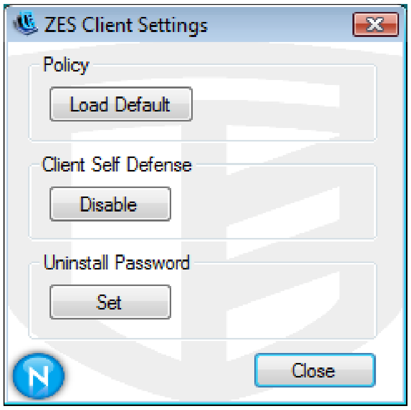
The client status includes information on the following objects:

- **Environment:** Information on the computer, user, and the present session.
- **Location Aware:** Information on the policy distinguishing the computer’s location and its adapter environment.
- **OS Adapter List:** Lists the communication elements for the computer hosting the client.
- **Network Status:** Whether the client is connected to a network and whether it is a wired, wireless, or a modem connection.
- **Firewall Enforcement:** The firewall the client is using and its present state.
- **Volume Management:** The devices and volumes that are presently found on the client.

Settings

The *Settings* button lets administrators adjust the settings for the Endpoint Security Client without reinstalling the software.

Figure 8-5 Endpoint Security Client Settings Control



The following sections contain more information:

- "Reset to Default Policy" on page 200
- "Disable Client Self Defense" on page 200
- "Set Uninstall Password" on page 200

Reset to Default Policy

Restores the original installed policy, whether that policy is a resource file or one that is distributed as part of the install package. Use this option if you need to access a policy with few or no restrictions enabled. This policy is permanent. To enforce a different policy, you must publish that policy to the client.

Disable Client Self Defense

Disables all protections used to keep the client installed and active on the machine.

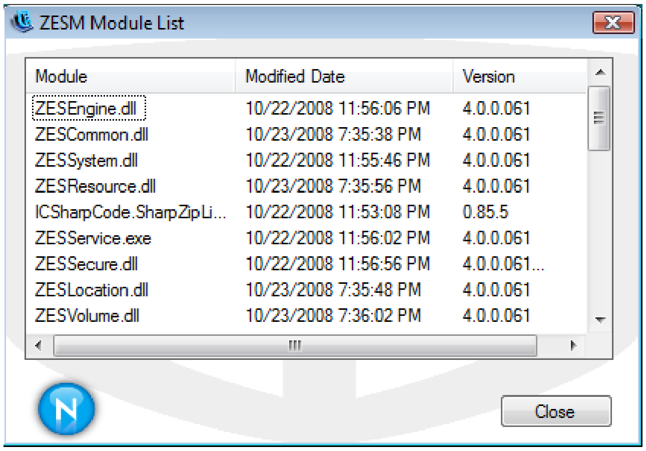
Set Uninstall Password

Resets the password required to uninstall the Endpoint Security Client. If no uninstall password is presently set, the administrator is prompted with a window to enter the uninstall password. When the password is set, the *Set* button becomes *Reset* and a *Remove* button is added. Use *Reset* to change the uninstall password, and use *Remove* to clear the uninstall password.

8.4.3 Module List

The *Module List* option shows all of the ZENworks Endpoint Security modules that are presently loaded on the client machine. To get to the Module List, double-click the Endpoint Security Client icon in the notification area to bring up ZENworks Endpoint Security Client About window, then click *Diagnostics > Module List*.

Figure 8-6 *Module List*



Module	Modified Date	Version
ZESEngine.dll	10/22/2008 11:56:06 PM	4.0.0.061
ZESCommon.dll	10/23/2008 7:35:38 PM	4.0.0.061
ZESSystem.dll	10/22/2008 11:55:46 PM	4.0.0.061
ZESResource.dll	10/23/2008 7:35:56 PM	4.0.0.061
ICSharpCode.SharpZipLi...	10/22/2008 11:53:08 PM	0.85.5
ZESService.exe	10/22/2008 11:56:02 PM	4.0.0.061
ZESSecure.dll	10/22/2008 11:56:56 PM	4.0.0.061...
ZESLocation.dll	10/23/2008 7:35:48 PM	4.0.0.061
ZESVolume.dll	10/23/2008 7:36:02 PM	4.0.0.061

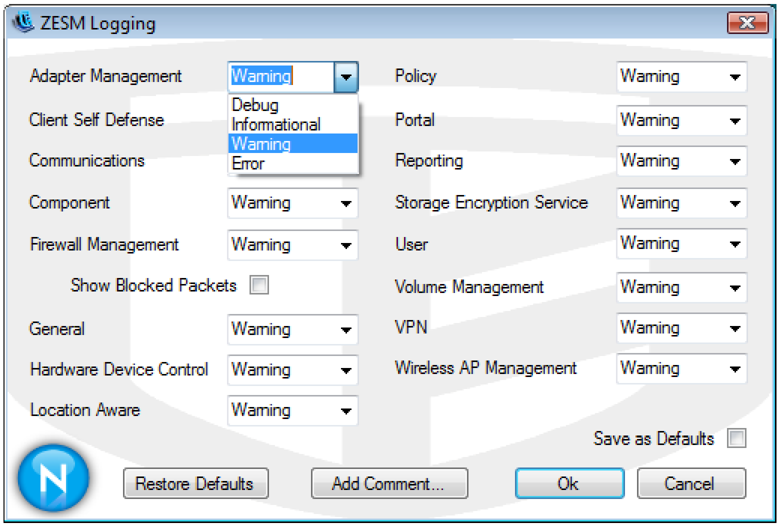
The Module List window displays all of the modules that are presently loaded on the client machine, the date the module was last modified, and the module's version number. Use this information to check this client's version for diagnostic purposes.

Click the *Module*, *Modified Date*, and *Version* headings to toggle names, dates, and versions. Click *Close* to close the Module List window.

8.4.4 Logging

Logging can be turned on for the Endpoint Security Client, permitting it to log specific system events. Log files are saved in the `C:\users\allusers\novell\ZES\log` directory (this is a hidden folder, so you will need to change the folder options to see the folder). To turn on and configure logging, double-click the Endpoint Security Client icon in the notification area to bring up ZENworks Endpoint Security Client About window, then click *Diagnostics* > *Logging*.

Figure 8-7 *Logging Window*



Adapter Management	Warning	Policy	Warning
Client Self Defense		Portal	Warning
Communications		Reporting	Warning
Component	Warning	Storage Encryption Service	Warning
Firewall Management	Warning	User	Warning
Show Blocked Packets	□	Volume Management	Warning
General	Warning	VPN	Warning
Hardware Device Control	Warning	Wireless AP Management	Warning
Location Aware	Warning		

Save as Defaults □

By default, all logging events are set to *Warning*, but you can set each listed event to the following:

- **Debug:** Turns on every possible message and includes Informational, Warning and Error messages.
- **Informational:** Records all events when they occur, such as when a network connection event begins and ends.
- **Warning:** Records errors that have occurred but are solvable and do not prevent the client from running.
- **Error:** Records errors that have occurred and prevent the client from running.

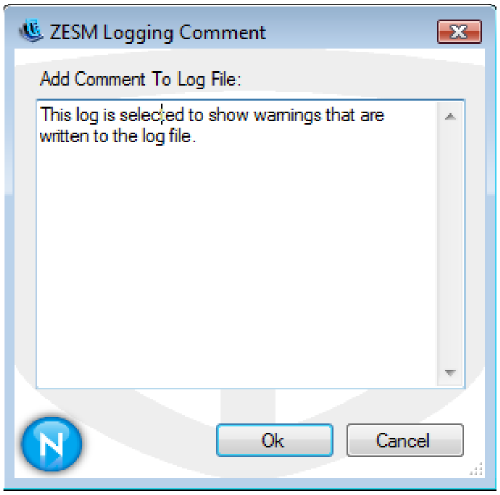
Use the *Save as Defaults* button to save a particular configuration. The configuration is then saved to the `C:\users\allusers\novell\ZES\log` directory, where it can be used the next time you select *Logging*. Select *Restore Defaults* to restore the Logging window to its default state (all events to *Warning* if *Save as Defaults* is not selected), or to the state when you selected *Save as Defaults*.

When troubleshooting, it is recommended that you set logging according to the directions of Novell Support and recreate the circumstances that led to the error to see if it can be repeated.

Add Comment

The option to add a comment to the logs is available in the Logging window. Click the *Add Comment* button to display the Logging Comment window. Comments are included with the next batch of logs.

Figure 8-8 *Comment Window*



This log is selected to show warnings that are written to the log file.

Using ZENworks Endpoint Security Management Utilities

9

Novell ZENworks Endpoint Security provides the following utilities to help you manage your environment:

- Section 9.1, "Using the ZENworks File Decryption Utility," on page 203
- Section 9.2, "Using the Override-Password Key Generator," on page 204

9.1 Using the ZENworks File Decryption Utility

The ZENworks File Decryption Utility is used to extract protected data from the Password Encrypted Files folder on encrypted removable storage devices. You must provide this utility to users; it is not part of the Security client. The utility cannot be placed on the encrypted removable storage device.

The utility (`stdecrypte.exe`) is located on the ZENworks Endpoint Security Management media in the `*language*\tools\stdecrypt_novell` directory.

The following sections contain more information:

- Section 9.1.1, "Using the File Decryption Utility," on page 203
- Section 9.1.2, "Using the Administrator Configured Decryption Utility," on page 204

9.1.1 Using the File Decryption Utility

To use the File Decryption Utility:

1. Plug the storage device into the appropriate port on your computer.
2. Open the File Decryption Utility (stdecrypt.exe).
3. Click the *Advanced* button.
4. In the Source panel, select *Password Protected Only*.
5. In the Source panel, click *Browse*, navigate to the storage device's Password Encrypted Files directory, select the desired file, the click *Save*.

   or

   To decrypt the entire Password Encrypted Files directory rather than a single file, select *Directories*, then browse to and select the directory.
6. In the Destination panel, click *Browse* to select the folder on the local machine where the decrypted files will be stored.
7. Click *Decrypt*.
8. Enter the password to decrypt the file.

   If you selected the entire directory, it is possible that all files do not have the same password. You are prompted each time the utility attempts to open a file that has a different password.

The transaction can be monitored by clicking the *Show Progress* button.

9.1.2 Using the Administrator Configured Decryption Utility

The File Decryption Utility can also be configured in administrator mode with the current key set, and can extract all data from an encrypted storage device. This configuration is not recommended, as it can potentially compromise all current keys used by the ZENworks Storage Encryption Solution. However, in cases where the data is otherwise unrecoverable, this configuration may be necessary.

To configure the tool:

1. Create a shortcut for the File Decryption Utility within its current directory.
2. Right-click the shortcut, then click *Properties*.
3. At the end of the target name, and after the quotes, enter `-k` (example: "C:\Admin Tools\stdecrypt.exe" -k).
4. Click *Apply*, then click *OK*.
5. Open the tool using the shortcut, then click *Advanced*.
6. Click the *Load Keys* button to open the Import Key window.
7. Browse for the keys file and specify the password for the keys.

All files encrypted with these keys can now be extracted.

9.2 Using the Override-Password Key Generator

Productivity interruptions that a user may experience due to restrictions to connectivity, disabled software execution, or access to removable storage devices are likely caused by the security policy the Endpoint Security Client is enforcing. Changing locations or firewall settings most often lifts these restrictions and restores the interrupted functionality. However, in some cases the restriction could be implemented in such a way that they are restricted in all locations and firewall settings, or the user is unable to make a location or firewall setting change.

When this occurs, the restrictions in the current policy can be lifted via a password override to allow productivity until the policy can be modified. This feature allows an administrator to set up password protected override for specified users and functionality, which temporarily permits the necessary activities.

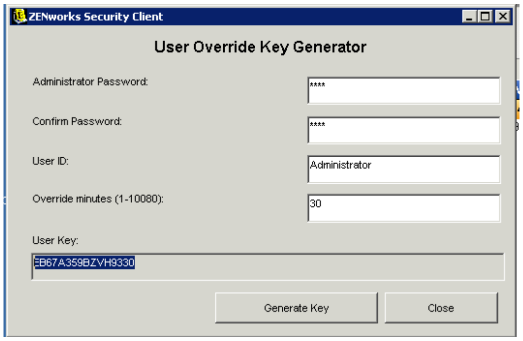
Password overrides disable the current security policy (restoring the default, All Open policy) for a pre-defined period of time, after the time-limit expires, the current or updated policy is restored. The password for a policy is set in the security policy's Global Rules settings.

Password override does the following:

- Overrides application blocking
- Allows users to change locations
- Allows users to change firewall settings
- Overrides hardware control (thumb drivers, CDROM, etc.)

The password entered into the policy should never be issued to an end user. It is recommended that the Override-Password Key Generator be used to generate a short-term-use key.

Figure 9-1 *Override Password Key Generator*



User Override Key Generator

Administrator Password: ****

Confirm Password: ****

User ID: Administrator

Override minutes (1-10080): 30

User Key: EB67A359BZVH9330

To generate an override key:

1. Click *Start* > *All Programs* > *Novell* > *ESM Management* > *Override-Password Generator*.
2. Specify the global policy password in the *Administrator Password* box, and confirm it in the next box.
3. Specify the local user logged in on the target machine.

   The username is case sensitive.
4. Specify the amount of time the policy should be disabled.
5. Click the *Generate Key* button to generate an override key.

This key can be either read to the end user during a help-desk call, or it can be copied and pasted into an e-mail message. To use the key, the user must open the About dialog box in the ZENworks Security Client, click the *Password Override* button, then enter the key. This key is valid for that user's policy only and only for the specified amount of time. Once the key has been used, it cannot be used again.

NOTE: If the user logs off or reboots the computer during password override, the password expires, and a new password must be issued.

If a new policy has been written prior to the time limit expiring, the end user should be instructed to check for a policy update, rather than clicking the *Load Policy* button in the ZENworks Security Client About dialog box.

Acronym Glossary

A

ACL	Access Control List
AP	Access Point
ARP	Address Request Protocol
CLAS	Client Locations Assurance Service
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DNS	Domain Name System
EAP	Extensible Access Protocol
ESM	ZENworks Endpoint Security Management
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FUS	Fast User Switching
HTTP	Hyper Text Transport Protocol
ICMP	Internet Control Message Protocol
IIS	Internet Information Service
LDAP	Lightweight Directory Access Protocol
LEAP	Light Extensible Access Control
LLC	Logical Link Control
MAC	Media Access Control
MMC	Microsoft Management Console
MSI	Microsoft Installer
NAC	Network Access Control
NDIS	Network Driver Interface Specification
NIC	Network Interface Card
PEAP	Protected Extensible Authentication Protocol
RAS	Remote Access Service
RDBMS	Relational Database Management System
RPC	Remote Procedure Call
RSSI	Received Signal Strength Indication
SES	Storage Encryption Solution

SNAP	Scalable Node Address Protocol
SNR	Signal to Noise Ratio
SQL	Structured English Query Language
SSID	Service Set Identifier
SSL	Secure Socket Layering
SUS	Microsoft Software Update Services
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WLAN	Wired Local Area Network
WPA	Wi-Fi Protected Access
ZSC	ZENworks Security Client