AUTHORIZED DOCUMENTATION

Administration Guide

Novell®
ZENworks® Endpoint Security Management

4.1

February 4, 2010

www.novell.com

Legal Notices

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

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

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

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

This *Novell® ZENworks® Endpoint Security Management Administration Guide* provides information to help you manage the Endpoint Security Management services, create and publish security policies, and generate and analyze reporting data.

The information in this guide is organized as follows:

- Part I, “System Configuration and Maintenance,” on page 13
- Part II, “Security Policies,” on page 37
- Part III, “Security Client,” on page 105
- Part IV, “Auditing,” on page 137
- Part V, “Utilities,” on page 161
- Part VI, “Appendixes,” on page 169

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 4.1 documentation Web site (http://www.novell.com/documentation/zesm41).

Documentation Conventions

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

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

System Configuration and Maintenance

I

The following sections contain information to help you configure and maintain your ZENworks® Endpoint Security Management system.

Managing Directory Service Connections

1

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

The following sections provide information to help you manage directory service configurations:

- Section 1.1, “Creating a Directory Service Configuration,” on page 15
- Section 1.2, “Synchronizing the Management Database with the Directory Service,” on page 21
- Section 1.3, “Removing a Directory Service Configuration,” on page 21

1.1 Creating a Directory Service Configuration

When you create a directory service configuration for a directory, you define the connection information for the Management Service to access the directory and identify the users or computers to whom policies can be published.

If necessary, you can create multiple directory service configurations to support publishing of policies to users or computers in different directories.

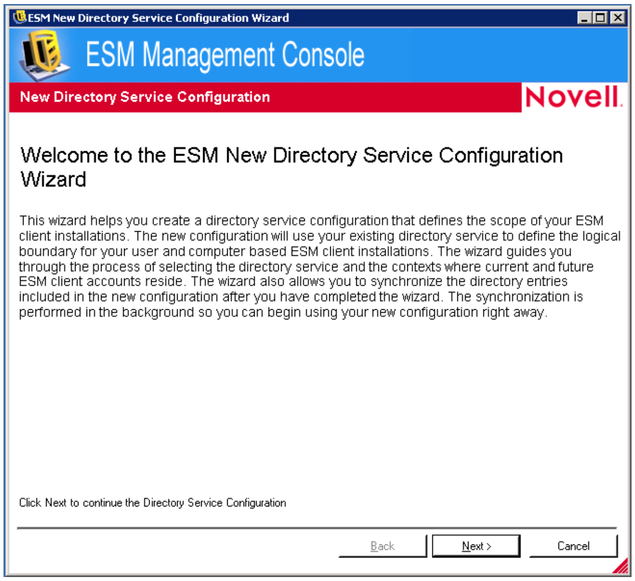
The following sections provide instructions for creating configurations for the two directory services:

- Section 1.1.1, “Defining eDirectory as the Directory Service,” on page 15
- Section 1.1.2, “Defining Active Directory as the Directory Service,” on page 18

1.1.1 Defining eDirectory as the Directory Service

1 In the Management Console, make sure the New Directory Service Configuration Wizard is displayed.

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



New Directory Service Configuration

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

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

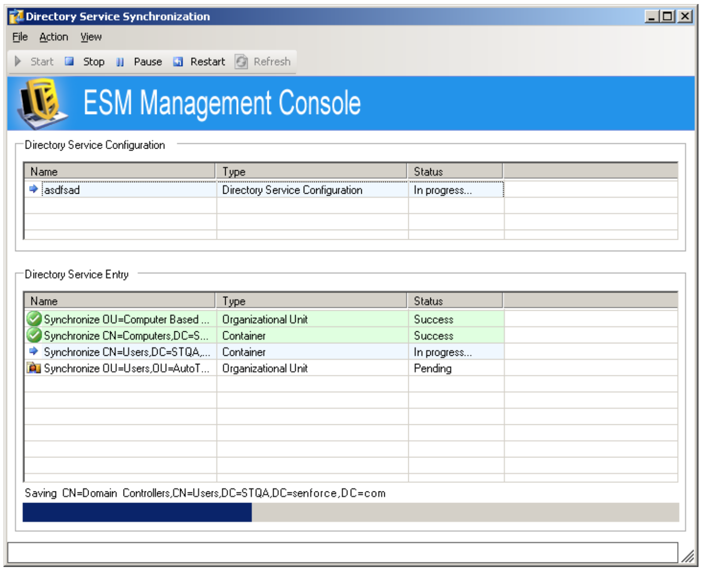
Wizard Page	**Explanation**
Configure Server	Select *Novell eDirectory*. In the *Name* field, specify a name that identifies this configuration in the Management Console. When users log in through the Security Client, the must select the directory service configuration that represents the directory service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

Wizard Page	Explanation
Select Directory Partition(s)	To receive security policies, the Security client must authenticate to eDirectory through a user or workstation account. You must identify the location of the users or workstations that you want to be able to authenticate. The first step is to select the partitions that contain the users or workstations.
Select Client Context(s)	The second step in identifying the location of the users or workstations that you want to be able to authenticate is to select the containers in which the users or workstations reside.
Select Context(s) for Synchronization	To publish a security policy to a user or workstation, the user or workstation must be available in the Management Console. There are two ways a user or workstation becomes available in the console: ◆ You use this page to synchronize the Management Console with eDirectory. To do so, select the eDirectory containers with users or workstations you want to populate into the Management Console. You can synchronize only the containers you selected as Client contexts (the previous page). ◆ Wait for the user or workstation to authenticate through the Security Client. When the user or workstation checks in, it is automatically added to the Management Console. Synchronizing containers prepopulates the Management Console so that you can immediately publish security policies to individual users or workstations. If you don't synchronize containers, you must publish security policies at the container level (which means all users or workstations in the container receive the policies) or wait for individual users or workstations to authenticate and be added to the Management Console.

3 If you have not already done so, click *Finish* to complete the directory service configuration.

The directory is added to the *Directory Service Configurations* list.

If you selected containers to synchronize, the Management Console begins the synchronization. You can double-click 🔄 in the Windows* notification area to display the Directory Services Synchronization dialog box.


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

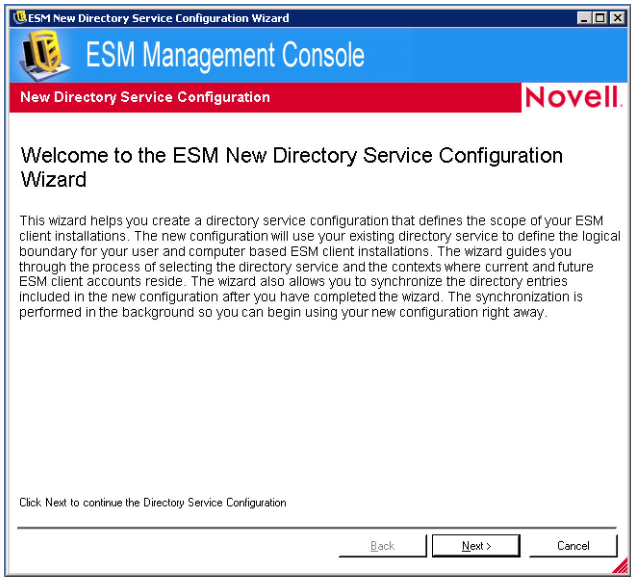
Saving CN=Domain Controllers,CN=Users,DC=STQA,DC=senforce,DC=com

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.

1.1.2 Defining Active Directory as the Directory Service

1 In the Management Console, make sure the New Directory Service Configuration Wizard is displayed.

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


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

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

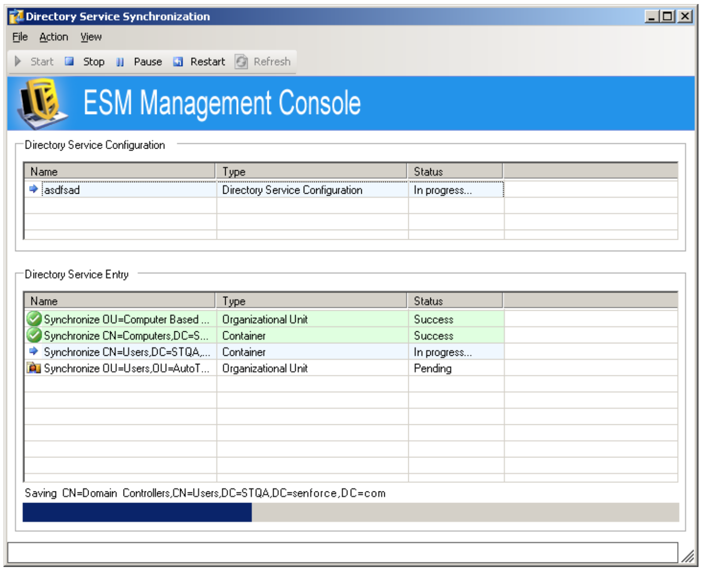
Wizard Page	Explanation
Configure Server	Select *Microsoft Active Directory*. In the *Name* field, specify a name that identifies this configuration in the Management Console. When users log in through the Security Client, the must select the directory service configuration that represents the directory service in which their user account exists. If you will have multiple directory service configurations, we recommend that the names you provide for the configurations are the same as or similar to the Active Directory domain names so that users recognize which configuration to select.
Connect to Server	**Host Name:** Specify the DNS name or IP address of an Active Directory server. By default, the field is populated with the address of an Active Directory server in the Management Console’s domain. To select a different Active Directory server, click *Browse*. **Port:** 3268 (the default) is the Active Directory Global Catalog server port. If the specified Active Directory server is not a Global Catalog server, specify a different port (for example, 389). **Enable Encryption:** Select this option if you want to use either Kerberos* or NTLM to encrypt the current session. Encrypting the session ensures that the Active Directory data imported by the Management Console is secure during transmission.
Provide Credentials	The Management Console requires a user account for authentication to Active Directory. **User Name:** Specify the login name of a user who has permission to view the entire directory. We recommend that you use the domain administrator. **Password:** Specify the password for the user account. **Domain:** Select the user’s domain. **Authentication Method:** Select the authentication method required by the Active Directory server (*Basic*, *Kerberos*, *NTLM*, *Negotiate*).
Locate Account Entry	This page is displayed only If the administrator account you specified is not in a standard Active Directory user container. Expand the directory tree to locate and select the administrator’s container.
Select Authenticating Domain(s)	To receive security policies, the Security client must authenticate to Active Directory through a user or computer account. You must identify the location of the users or computers that you want to be able to authenticate. The first step is to select the domains that contain the users or computers.
Select Client Container(s)	The second step in identifying the location of the users or computers that you want to be able to authenticate is to select the containers in which the users or computers reside.

Wizard Page	Explanation
Select Container(s) for Synchronization	To publish a security policy to a user or computer, the user or computer must be available in the Management Console. There are two ways a user or computer becomes available in the console: ◆ You use this page to synchronize the Management Console with Active Directory. To do so, select the Active Directory containers with users or computers you want to populate into the Management Console. You can synchronize only the containers you selected as Client containers (the previous page). ◆ Wait for the user or computer to authenticate through the Security Client. When the user or computer checks in, it is automatically added to the Management Console. Synchronizing containers prepopulates the Management Console so that you can immediately publish security policies to individual users or computers. If you don't synchronize containers, you must publish security policies at the container level (which means all users or computers in the container receive the policies) or wait for individual users or computers to authenticate and be added to the Management Console.

3 If you have not already done so, click *Finish* to complete the directory service configuration.

The directory is added to the *Directory Service Configurations* list.

If you selected containers to synchronize, the Management Console begins the synchronization. You can double-click in the Windows notification area to display the Directory Services Synchronization dialog box.



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.

1.2 Synchronizing the Management Database with the Directory Service

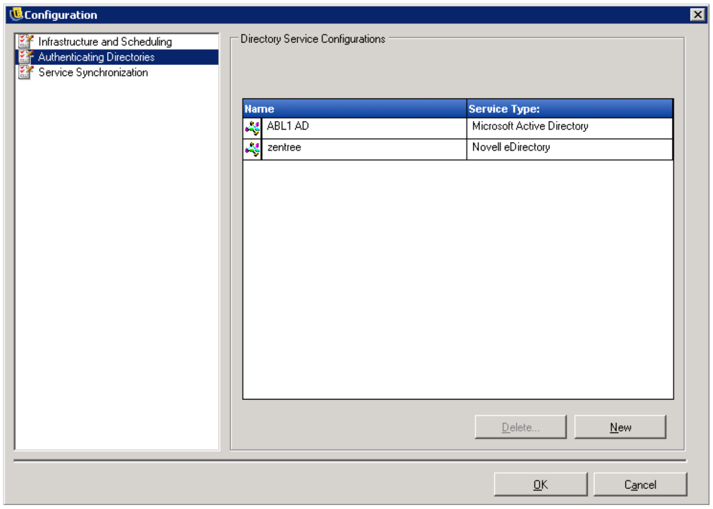
By default, the Management Service synchronizes the Management database with the directory service every 4 hours. If necessary, you can change the synchronization schedule. For instructions, see Chapter 3, “Configuring Data Synchronization Schedules,” on page 25.

1.3 Removing a Directory Service Configuration

When you remove a directory service configuration from your system, the following occurs:

- Any users and computers that authenticate through the directory service configuration no longer receives policy updates.
- The same users and computers are no longer able to submit report data to the system. During the deletion process, you can choose to retain or remove the currently stored reporting data for these users and computers.

1. In the Management Console, click the *Tools* menu, then click *Configuration* to display the Configuration dialog box.
2. Click *Authenticating Directories*.


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

Name	Service Type:
ABL1 AD	Microsoft Active Directory
zentree	Novell eDirectory

3. In the *Directory Service Configurations* list, select the configuration you want to delete, then click *Delete* to launch the Delete Directory Services Configuration Wizard.
4. Follow the prompts to delete the directory service configuration.

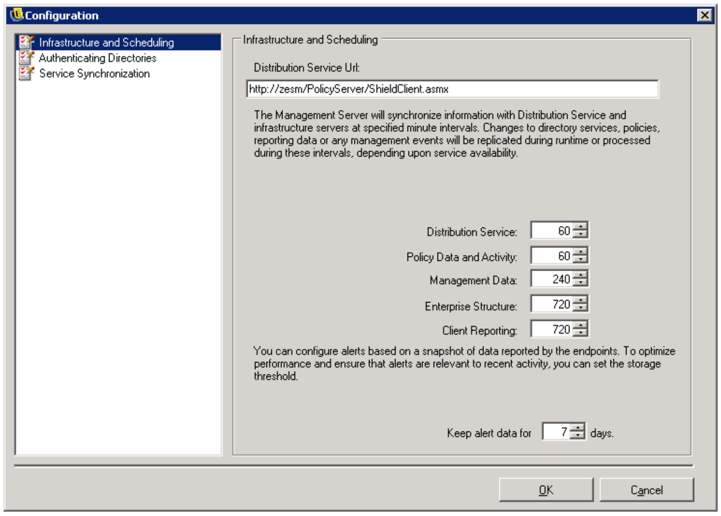
Changing the Policy Distribution Service URL

2

Both the Management Service and the Security Clients must know the URL of the Policy Distribution Service. If you move the Policy Distribution Service to a new server or change the address of the current server, you need to change the URL in the Management Console.

1 In the Management Console, click the *Tools* menu, then click *Configuration* to display the Configuration dialog box.

2 Click *Infrastructure and Scheduling*.


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.

3 In the *Distribution Service URL* field, change the server name.

Change only the server name. Do not change any information after the server name. For example, 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`.

4 Click *OK*.

The Management Service and all policies are updated with the new location.

You should not terminate the old Policy Distribution Service until the updated policies have a 100 percent adherence level. For more information about adherence reports, see Section 21, "Generating Standard Reports," on page 139.

Configuring Data Synchronization Schedules 3

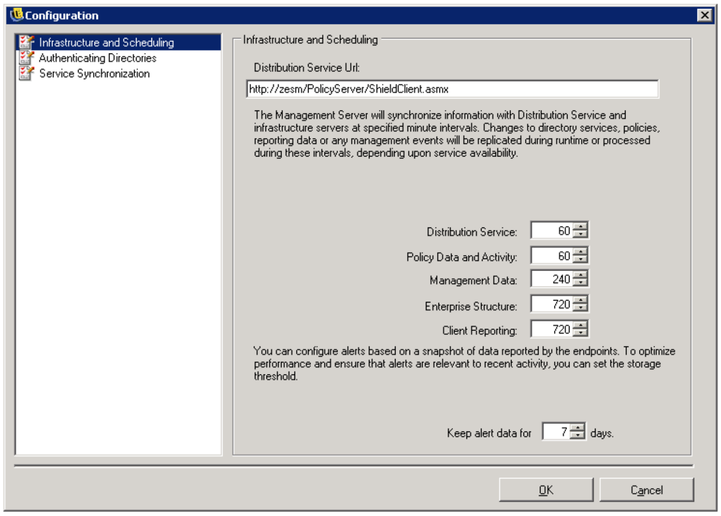
The ZENworks® Endpoint Security Management system requires synchronization of data (policies, reports, alerts, directory service data, and so forth) among its various components. The system provides a default schedule for the synchronization of the various data types. If the default schedule is not meeting your needs, you can modify the schedule.

If necessary, you can initiate a synchronization of report, alert, and policy data. For information, see Chapter 4, "Forcing Data Synchronization," on page 27.

To configure the synchronization schedules:

1 In the Management Console, click the *Tools* menu, then click *Configuration* to display the Configuration dialog box.

2 Click *Infrastructure and Scheduling*.


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.

3 Change the following synchronization schedules as desired. All schedules are in minutes, with the exception of the alert data schedule, which is in days.

- **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 directory service (eDirectory™ or Active Directory). 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 checks 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 set the storage threshold based on a number of days.

4 Click *OK*.

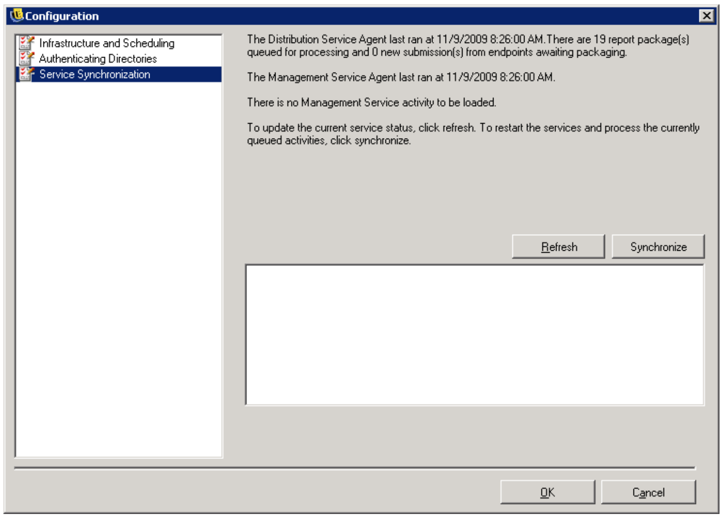
Forcing Data Synchronization

4

You can force a synchronization of the Management Service and Policy Distribution Service to update all alerting, reporting, and policy distribution data.

To force synchronization:

1. In the Management Console, click the *Tools* menu, then click *Configuration* to display the Configuration dialog box.
2. Click *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.

3. Click *Synchronize* to synchronize the two services and update the alerts, reports, and policy data.
4. Click *OK*.

Managing Directory Service Objects that Have Moved

5

When you add or delete a user or computer from your directory service, that change is reflected in your Management database after the next scheduled directory service synchronization (see Chapter 3, “Configuring Data Synchronization Schedules,” on page 25).

However, when you move a user or computer from one container to another in the directory service, that change is not reflected in your Management database. This means that the object remains in the same location in your Management Console tree even though its location has changed in the directory service.

Overall, this does not affect policy management or authentication for the moved user or computer. You can republish policies to the object and the object can still authenticate. The only difference is the display location in the Management Console and the directory service.

To resolve this issue so that moved objects display in the correct location in your Management Console tree:

1. Delete your directory service configuration. For instructions, see Section 1.3, “Removing a Directory Service Configuration,” on page 21.
2. Add the directory service configuration again. For instructions, see Section 1.1, “Creating a Directory Service Configuration,” on page 15.

The directory service configuration is completely removed from the Management database, added again, and synchronized with all objects in the correct contexts.

6 Renewing ZENworks Endpoint Security Management Credentials

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

Cryptographic best practices dictate that the credential, or key management key (KMK), be renewed at regular intervals to prevent certain cryptographic attacks from being practical. This can take place on a relatively long cycle, typically about once every year, and should not be done too frequently because the renewal requires some effort and network bandwidth.

To renew the KMK:

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

   Allow the Communications Console to run a complete check. Running the Communications Console causes the Management Service to lose user and log data; however, policy data is not deleted.

2. Have all end users authenticate to the Management Service (either via VPN or while inside the appropriate firewall) by right-clicking the Security Client taskbar icon, then clicking *Check for Policy Update*.

   The Management Service passes the new KMK credentials down. In some cases, the user must authenticate to the domain (username and password).

   Until the endpoints renew their KMKs, they cannot communicate with the Policy Distribution Service.

Managing Encryption Keys

7

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 data can be decrypted if there is a systems failure or an inadvertent policy change. 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.

The following sections contain additional information:

- Section 7.1, “Exporting Encryption Keys,” on page 33
- Section 7.2, “Importing Encryption Keys,” on page 33
- Section 7.3, “Generating a New Key,” on page 34

7.1 Exporting Encryption Keys

For backup purposes, or 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.

7.2 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*.

7.3 Generating a New Key

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

All previous keys are stored in the policy.

8 Applying a License Key

You can evaluate ZENworks® Endpoint Security Management for 60 days, after which you must apply a license key to continue using the product. You receive the license key from Novell when you purchase the product or request an evaluation extension.

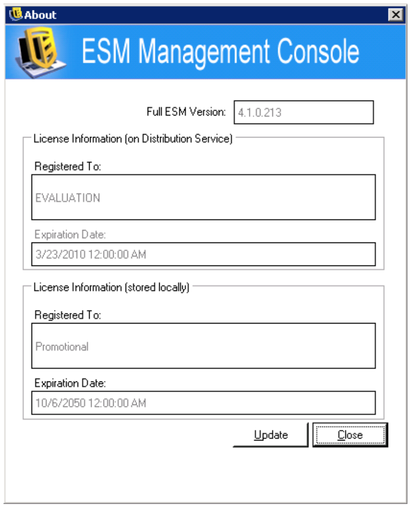
To apply the license key:

1 Copy the license key (`license.dat`) to the following folder on the Management Console machine:

   `\Program Files\Novell\ESM Management Console`

2 Log in to the Management Console.

3 Click the *Help* menu > *About Management Console*.



Full ESM Version: 4.1.0.213

License Information (on Distribution Service)

Registered To: EVALUATION

Expiration Date: 3/23/2010 12:00:00 AM

License Information (stored locally)

Registered To: Promotional

Expiration Date: 10/6/2050 12:00:00 AM

4 Click *Update*.

   The system is updated to the new license. In addition, the license is uploaded to the Policy Distribution Service. This enables Security Clients to receive the license the next time they check in.

   If you have unmanaged Security Clients (clients that do not check in for policy updates), you must manually distribute the license to the clients. Copy the `license.dat` file to the endpoint's `\Program Files\Novell\ZENworks Security Client` directory, then reboot the endpoint to activate the license.

Security Policies

II

The Security Client uses security policies to determine security enforcement on endpoint devices.

You can create security policies for your entire organization, specific groups, or individual users or machines. A security policy can allow full employee productivity while securing the endpoint, or it can restrict employees to running only certain applications and having only authorized hardware available to them.

Creating a Security Policy

9

A security policy consists of global settings, location-specific settings, integrity rules, and compliance reporting settings:

- **Global settings:** Global security settings are applied regardless of the endpoint device's location. Some global settings determine general Security Client behavior, such as whether or not Client Self Defense is enabled or a password is required to uninstall the client. Other settings determine basic security policy, such as data encryption for fixed and removable drives.
- **Location-based settings:** Location-based security settings are applied based upon the endpoint device's current network environment. You can define multiple locations, such as Office, Home, and Airport, to provide the appropriate security at each locations. To define a location, you specify the network environment parameters (gateway servers, DNS servers, access points, etc.) that identify the location; when the endpoint device detects that its current location matches the defined location, the Security Client applies the security settings for that location.

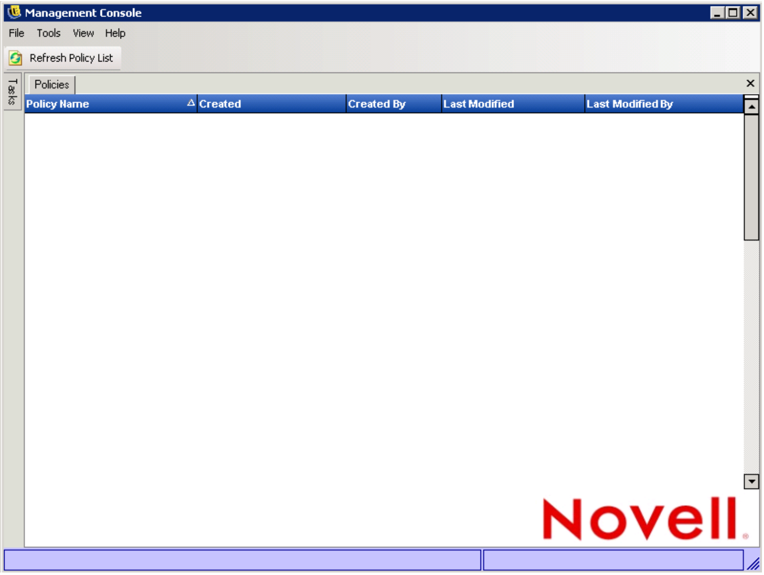
  You can use location-based settings to determine firewall security, wireless availability (including allowed access points, encryption security levels, and supported wireless adapters), communication hardware availability (IrDA, Bluetooth*, etc.), USB device connectivity, and storage device availability.

  Many of the components, such as locations, network environments, and firewalls are saved as individual components so that you can reuse them.
- **Integrity and Remediation Rules:** These rules provide the ability to verify that required software is running on the endpoint devices and then provide instant remediation procedures if the verification fails. For example, you might require that specific antivirus or spyware software be running.
- **Compliance Reporting:** The Security Client gathers extensive information about the endpoint device's activity. You can determine what information you want reported. For example, you can receive information about attempts to tamper with the Security Client, information about files copied to removable drives, and information about firewall activity. You can use this information to determine whether or not your security policies are configured correctly to enforce your organization's paper policies.

To create a security policy:

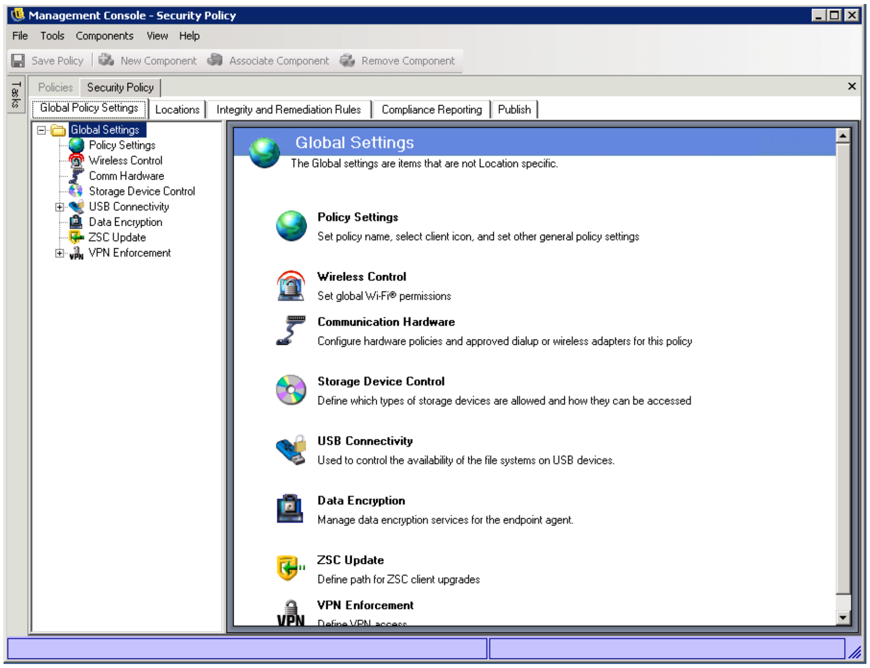
1. Launch the Management Console and log in.

   The Management Console launches with the *Policies* list displayed. Policies you create are listed here so that you can open and modify them as necessary.



2 Click *File* > *Create New Policy*.

3 Specify the name for the new policy, then click *Create*.



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

4 Configure and distribute the policy by referring to the information and instructions in the following sections:

- Chapter 10, "Configuring a Policy's Global Settings," on page 41
- Chapter 11, "Configuring a Policy's Locations," on page 61
- Chapter 12, "Configuring a Policy's Integrity and Remediation Rules," on page 87
- Chapter 13, "Configuring a Policy's Compliance Reporting," on page 97
- Chapter 14, "Distributing a Policy," on page 99

Configuring a Policy's Global Settings

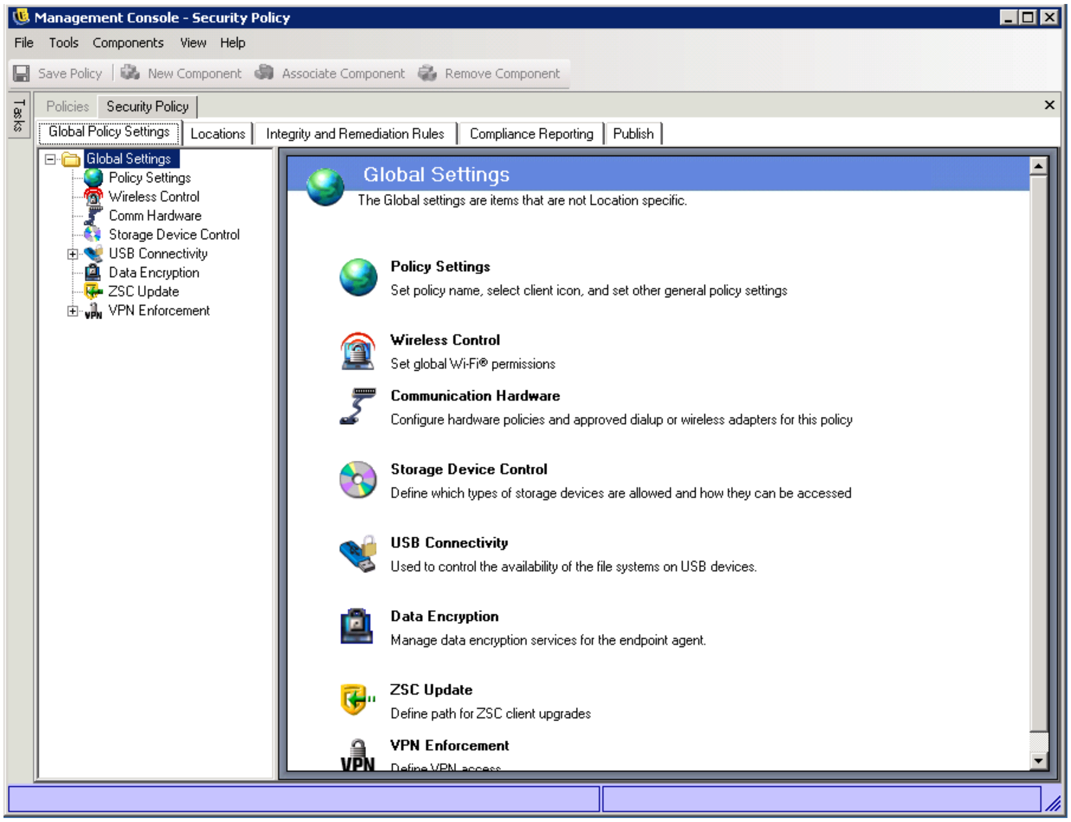
10

A policy includes global settings that are applied regardless of the endpoint device's location. Some global settings determine general Security Client behavior, such as whether or not Client Self Defense is enabled or a password is required to uninstall the client. Others determine basic security policy, such as data encryption for fixed and removable drives.

- Section 10.1, "Accessing the Global Settings," on page 41
- Section 10.2, "Policy Settings," on page 42
- Section 10.3, "Wireless Control," on page 44
- Section 10.4, "Communication Hardware," on page 46
- Section 10.5, "Storage Device Control," on page 47
- Section 10.6, "USB Connectivity," on page 49
- Section 10.7, "Data Encryption," on page 53
- Section 10.8, "ZSC Update," on page 56
- Section 10.9, "VPN Enforcement," on page 57

10.1 Accessing the Global Settings

1. In the Management Console, double-click the policy in the *Policies* list.
2. If it is not already selected, click the *Global Policy Settings* tab.



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 desired global settings by referring to the following sections:

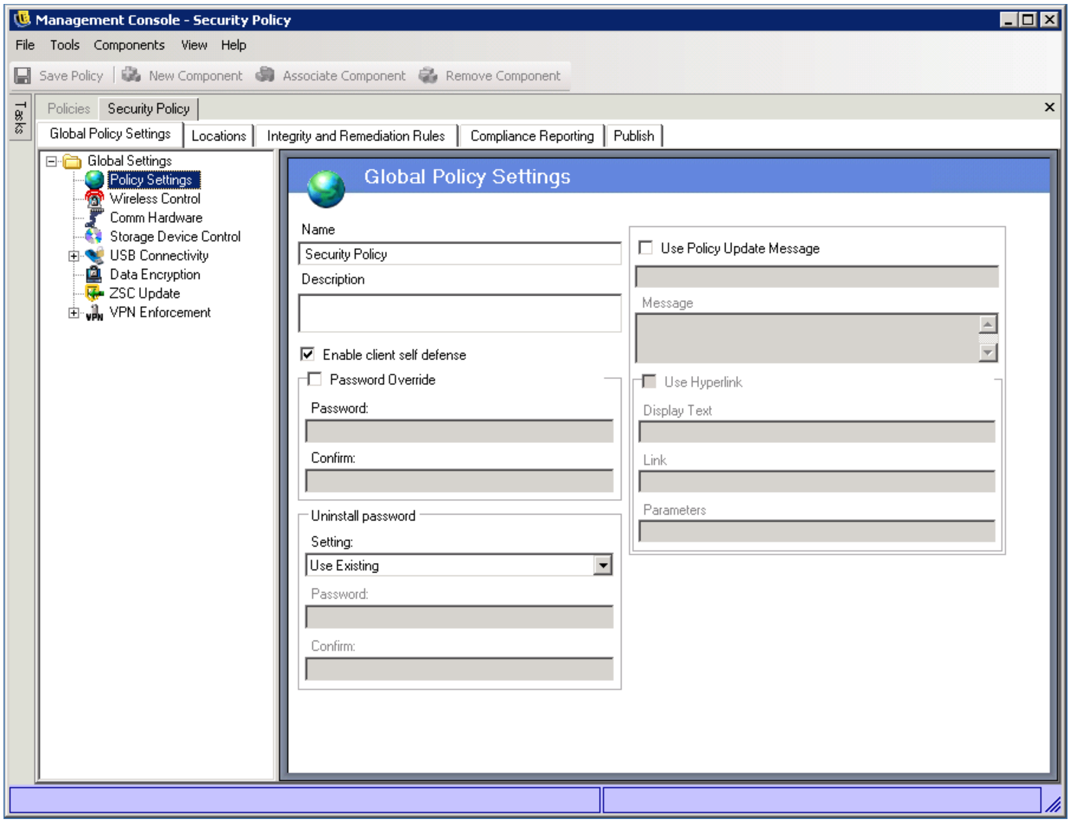
- "Policy Settings" on page 42
- "Wireless Control" on page 44
- "Communication Hardware" on page 46
- "Storage Device Control" on page 47
- "USB Connectivity" on page 49
- "Data Encryption" on page 53
- "ZSC Update" on page 56
- "VPN Enforcement" on page 57

10.2 Policy Settings

The Policy Settings include general settings for the Security Client. To configure the settings:

1 Make sure the policy you want to configure is open in the Management Console (see Section 10.1, "Accessing the Global Settings," on page 41).

2 On the *Global Policy Settings* tab, click *Policy Settings*.



Name: Security Policy

☑ Enable client self defense

□ Password Override

Uninstall password

Setting: Use Existing

□ Use Policy Update Message

□ Use Hyperlink

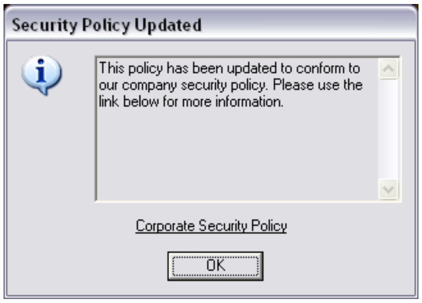
3 Configure the settings as desired:

- **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 temporarily disables the policy for a specified period of time. Select 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: End users should not be given this password. Instead, you should use the Override Password Generator to generate a temporary key for them.

- **Uninstall Password:** To effectively implement Client Self Defense, you need to control the uninstalling of the Security Client. We strongly recommend that every 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 a policy.
  - The default setting is *Use Existing*, which will not change the uninstall password specified at installation.

    - *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 the check box, then specify the message information in the provided boxes. The following is an example of the dialog box displayed to the user.



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

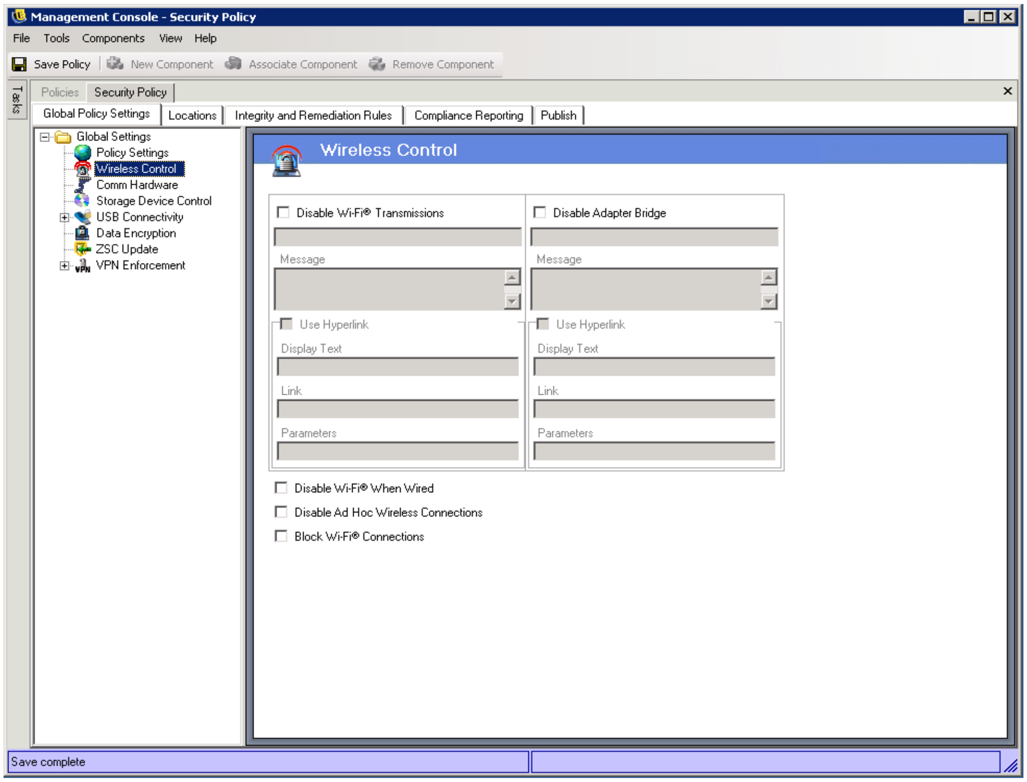
  - **Use Hyperlink:** You can include a hyperlink to additional information, corporate policy, or other related information at the bottom of the custom message.

4 Click *Save Policy* to save your changes.

10.3 Wireless Control

The Wireless Control settings determine the type of wireless functionality available. You can control such settings as whether or not wireless is enabled, whether or not it is enabled when a wired connection is available, and whether or not ad hoc wireless connections are allowed.

1. Make sure the policy you want to configure is open in the Management Console (see Section 10.1, "Accessing the Global Settings," on page 41).
2. On the *Global Policy Settings* tab, click *Wireless Control*.



3 Configure the settings as desired:

- **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.

  Wi-Fi transmissions are disabled without user notification. If you want to notify the user, you can choose to display a custom user message and hyperlink to the user if he or she attempts to activate a Wi-Fi connection.

- **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.

  Adapter bridging is disabled without user notification. If you want to notify the user, you can choose to display a custom user message and hyperlink to the user if he or she attempts to activate an adapter bridge.

  You can choose to display a custom user message and hyperlink when the user attempts a Wi-Fi connection.

- **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, enforcing Wi-Fi connectivity via an access point and restricting all peer-to-peer networking.

- **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 11, "Configuring a Policy's Locations," on page 61 for more information.

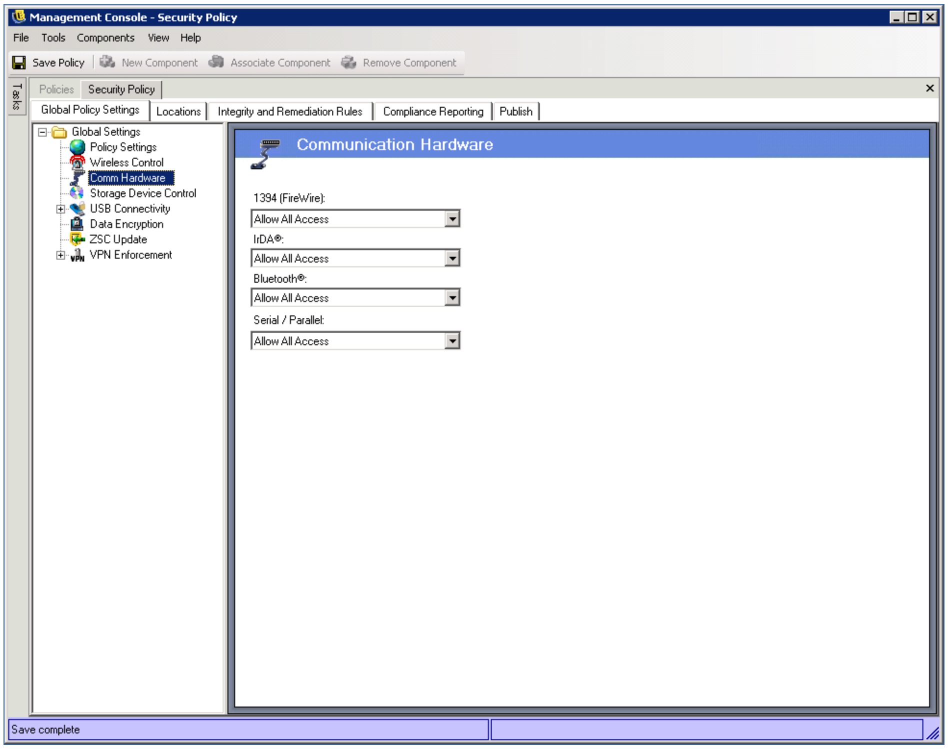
4 Click *Save Policy* to save your changes.

10.4 Communication Hardware

The Communication Hardware settings control which hardware types are permitted to have a connection.

1 Make sure the policy you want to configure is open in the Management Console (see Section 10.1, “Accessing the Global Settings,” on page 41).

2 On the *Global Policy Settings* tab, click *Communication Hardware*.



1394 (FireWire): Allow All Access

IrDA®: Allow All Access

Bluetooth®: Allow All Access

Serial / Parallel: Allow All Access

Save complete

3 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 on the endpoint.

  The Security Client can control access for most Widcom-based Bluetooth solutions. Supported devices include the following:

  - Devices using the Microsoft standard Type GUID {e0cbf06cL-cd8b-4647-bb8a263b43f0f974}
  - Devices using the Dell* USB Bluetooth module; the Dell Type GUID {7240100F-6512-4548-8418-9EBB5C6A1A94}
  - Devices using the HP*/Compaq* Bluetooth Module; the HP Type GUID {95C7A0A0L-3094-11D7-A202-00508B9D7D5A}

To determine if a Bluetooth device is one of the supported types listed above, open Regedit (on the endpoint device), navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class`, then search for the any of the GUID listed above. The Microsoft key must have more than one subkey to be valid.

- **Serial/Parallel:** Controls serial and parallel port access on the endpoint.

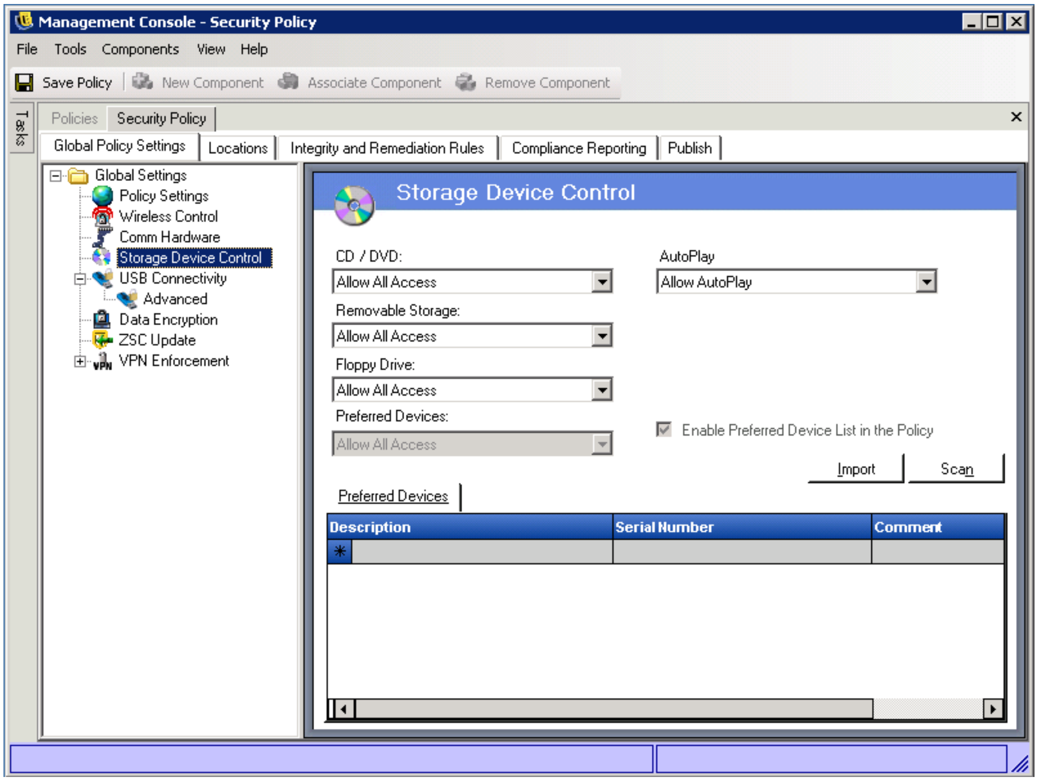
4 Click *Save Policy* to save your changes.

10.5 Storage Device Control

The Storage Device Control settings determine access to external storage devices (CD/DVDs, removable storage devices, and floppy drives). You can allow read/write access, read-only access, or no access. When disabled (no access), users cannot retrieve any data from the storage device; however, the hard drive and all network drives remain accessible and operational.

1 Make sure the policy you want to configure is open in the Management Console (see Section 10.1, "Accessing the Global Settings," on page 41).

2 On the *Global Policy Settings* tab, click *Storage Control Device*.



Storage Device Control

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
*		

3 For *CD/DVD*, *Removable Storage*, and *Floppy Drive*, select one of the following options:

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

- **Read-Only Access:** Read-only access is allowed. When users attempt to write to the device, they receive an error message from the operating system, or from the application attempting to access the local storage device, that the action has failed

CD/DVD controls all devices listed under *DVD/CD-ROM drives* in Windows Device Manager. *Removable Storage* controls all devices listed under *Floppy disk drives* in Windows Device Manager. *Floppy Drive* controls all devices listed under *Floppy disk drives* in Windows Device Manager.

To disable CD-ROM drives or floppy drives or set them as Read-Only, the endpoint device's Local Security Settings 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*. By default, these settings are disabled. If you need to disable them or verify that they are disabled, open either the Active Directory group policy object or open *Administrative Tools* on the target devices. Look in *Local Security Settings - Security Options* and verify that both settings are disabled.

4 For *Autoplay*, select from 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 specific content (music, video and pictures) is allowed.

The Windows AutoPlay feature 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.

5 If you want to restrict which removable storage devices are allowed, complete the following steps. Doing so creates a whitelist of devices that are allowed; any devices not included in the list are blocked.

5a In the *Preferred Devices* list, use one of the following methods to add the removable storage devices that you want to allow:

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

  Only the *Description* and *Serial Number* fields are used when matching devices. The *Comment* field is for your own information.

  The *Description* field is a partial match field. If you want to match multiple devices, use this field. For example, to match all SanDisk USB drives, enter SanDisk.

  The *Serial Number* field is an exact match field. Serial numbers are unique to specific removable storage devices. If you want to match specific devices, use this field.

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

  After the device information is scanned and displayed, you can edit the fields as necessary to create the device filter you want.

- Import device information from a file. To do so, click *Import*, select the file, then click *OK*. For information about creating an import file, see the *ZENworks Endpoint Security Management 4.1 Device Scanner Guide*.

5b Select the *Enable Preferred Device List in the Policy* setting.

This overrides the *Removable Storage* setting and activates the *Preferred Devices* list.

5c For the *Preferred Devices* setting, select one of the following access settings. All devices in the *Preferred Devices* list receive this access:

- **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 Access:** The devices on the *Preferred Devices* list are permitted read-only capability. All other Removable Storage devices are disabled.

6 Click *Save Policy* to save your changes.

10.6 USB Connectivity

The USB Connectivity settings control access to devices that connect via the USB bus. The settings provide control at several levels: all devices, device groups (classes), and individual devices. This gives you great flexibility in defining approved devices (whitelists) and prohibited devices (blacklists).

For example, assume that your organization supports only two authorized USB printers. You could allow access to all USB devices, block access to the printer device class, and then allow access to your two authorized printers. The result is a printer whitelist that includes only your two authorized printers.

- Section 10.6.1, “How the Access Setting Is Determined,” on page 49
- Section 10.6.2, “Configuring the USB Connectivity Settings,” on page 50

10.6.1 How the Access Setting Is Determined

To effectively use the USB Connectivity settings, you need to understand how the various settings are used to determine a device’s access.

When a device is detected, the first setting that is evaluated is the *USB Devices* setting. If the *USB Devices* setting is *Allow All Access*, the evaluation continues. If the setting is *Disable All Access*, the USB device is disabled and evaluation stops.

If the evaluation continues, the device’s attributes (Device Class, Manufacturer, Product, and so forth) are compared to the attributes associated with the device groups (in *Device Group Access*) and individual devices (in the device list on the *Advanced* page). In some cases, the device might match more than one group and device. For example, a removable storage device might match both the Mass Storage Class group and an individually defined device.

In order to know which access setting to apply to a USB device, the Security Client builds an access filter against which to evaluate devices. If multiple security policies apply, the Security Client uses the USB Connectivity settings from all applied policies to build the access filter.

The filter includes each access setting (*Always Block*, *Always Allow*, *Block*, *Allow*, and *Default Device Access*) and the device groups and devices assigned to the setting. For example, assume the following group and device assignments for each access setting:

Access Setting	Group Assignments	Device Assignment
Always Block		Mouse1
		Thumbdrive2, Thumbdrive5
Always Allow	Human Interface Device	Printer4, Printer3, Printer1
Block	Printing Class	Scanner1
Allow	Mass Storage Class	Printer2
	Scanning/Imaging (PTP	

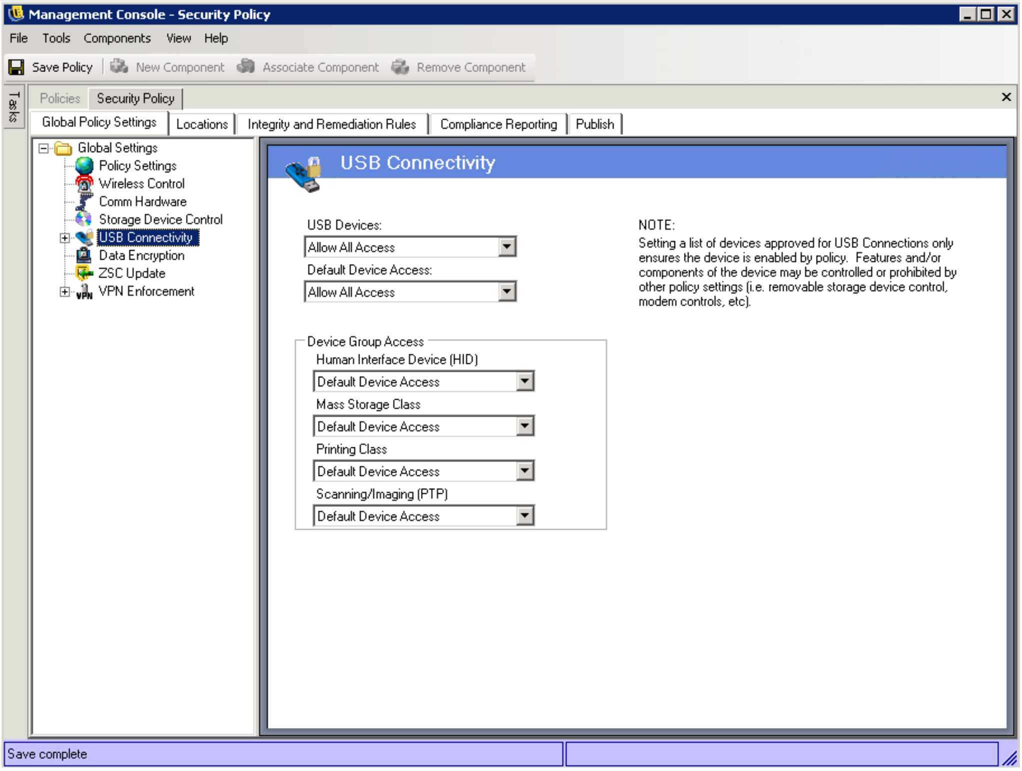
A USB device is evaluated against the filter, beginning with the first setting (*Always Block*) and continuing to the last (*Allow*). If the device matches one of the device groups or devices assigned to the access setting, the device receives that access setting and the evaluation ends. If a device does not match any of the groups or devices, it receives the default device access.

Consider the following examples:

- Mouse1(a Human Interface Device) is detected. It is evaluated against the first setting (*Always Block*). Because Mouse1 matches the Mouse1 device assignment for the *Always Block* setting, Mouse1 is blocked and no further evaluation is required.
- Mouse4 (a Human Interface Device) is detected. It is evaluated against the *Always Block* setting. Mouse4 does not match any *Always Block* assignments (group or device), so it is evaluated against the *Always Allow* assignments. Because Mouse4 is a Human Interface Device and that device group is assigned the *Always Allow* setting, Mouse4 is allowed and no further evaluation is required.
- Thumbdrive1 and Thumbdrive5 (two Mass Storage Class devices) are detected. Thumbdrive5 is blocked because its device assignment (*Always Block*) precedes its Mass Storage Class group assignment (*Allow*). Thumbdrive1 is allowed because it is included in the Mass Storage Class group assignment (*Allow*) and it does not match a device assignment.
- Printer2 and Printer4 (two Printing Class devices) are detected. Printer4 is allowed because its device assignment (*Always Allow*) precedes its Printing Class group assignment (*Block*). Printer2 is blocked because its Printing Class group assignment precedes its device assignment (*Allow*).

10.6.2 Configuring the USB Connectivity Settings

1. Make sure the policy you want to configure is open in the Management Console (see Section 10.1, "Accessing the Global Settings," on page 41).
2. On the *Global Policy Settings* tab, click *USB Connectivity*.



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

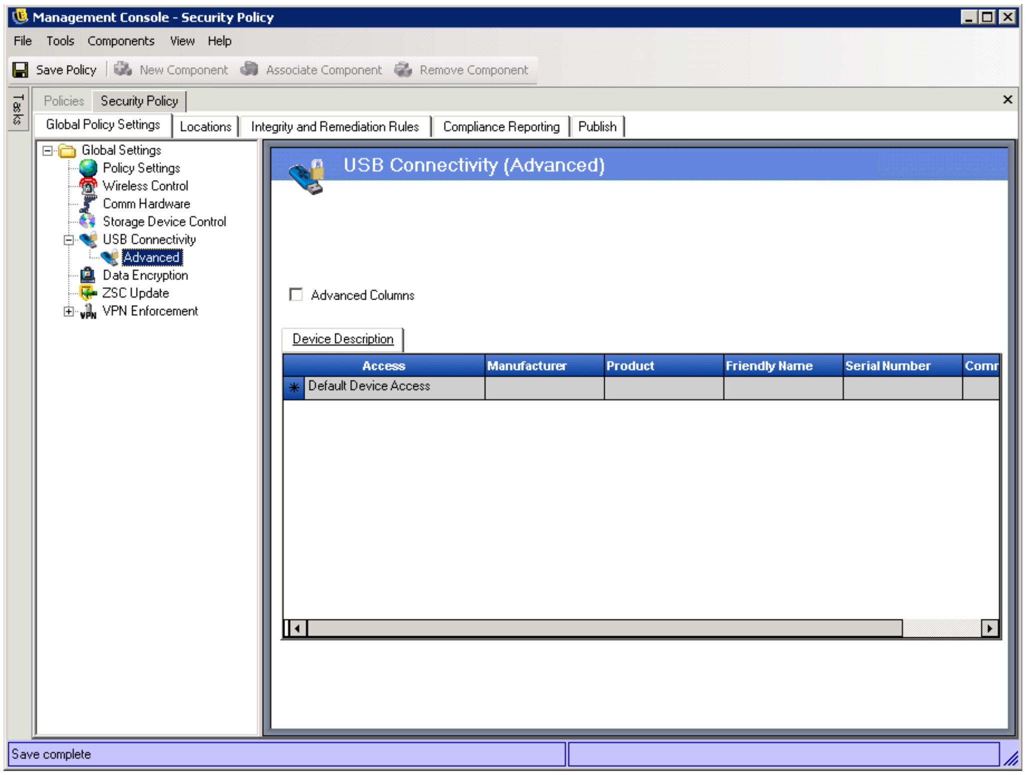
3 Configure the settings as desired:

- **USB Devices:** Device access is first evaluated based on whether the USB bus is active or not. 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 Security Client continues the evaluation based on the remaining settings.
- **Default Device Access:** Select the default access (*Allow All Access* or *Disable All Access*) that will be assigned to USB devices in the following situations:
  - A USB device does not match one of the defined device groups or devices.
  - A USB device matches a defined device group or device whose access is set to *Default Device Access*.
- **Device Group Access:** For each device group listed, select the access you want assigned to the group:
  - **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.

The device groups are determined by the following classes. If a USB device's class corresponds to one of the groups, it receives the group's assigned access.

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.

4 If you want to define individual devices, click the plus sign next to *USB Connectivity* in the *Global Settings* tree, then click *Advanced*. Otherwise, skip to Step 7 on page 53.



Access	Manufacturer	Product	Friendly Name	Serial Number	Comr
Default Device Access					

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.

5 To add a device to the list, fill in the device fields.

The device fields create a filter against which detected devices are compared. The detected device's attributes must match all device fields defined for the filter. For example, assume that you define a device using the following fields:

- Manufacturer=Acme

- Device Class=8
- Serial Number=1234

To match the filter, a detected device must have a Manufacturer attribute that contains Acme (Manufacturer is a substring match field), a Device Class attribute that equals 8, and a Serial Number attribute that equals 1234.

If the detected device does not provide an attribute that is required by the filter, the match fails. For example, a detected device without a Serial Number equal to 1234 would not match.

Fill in the following fields to define the device filter and the access assigned to devices that match the filter:

- **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* filter 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, such as Canon. This is a substring match field, meaning that both *C* and *Can* would match *Canon*.
- **Product:** Click the *Product* column, then type the name of the product. This is a substring match field, meaning that both *C* and *Can* would match *Canon*.
- **Friendly Name:** Click the *Friendly Name* column then type the friendly name of the device. This is a substring match field, meaning that both *C* and *Can* would match *Canon*.
- **Serial Number:** Click the *Serial Number* column, then type the serial number of the device. Be aware that not all USB devices have unique serial numbers. To guarantee a unique match based on serial number, you must also use the *USB Version*, *Vendor ID*, *Production ID*, and *BCD Device* fields. *Serial Number* is an exact match field.
- **Comment:** Click the *Comment* column, then type a comment. This field is not used to match devices, so it can include any text you want.

6 If you want to use additional attributes to define the device, click *Advanced Columns*.

This adds 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*.

All fields are exact match fields. Current valid values for the USB version in decimal are 512 - USB 2.0, 272 - USB 1.1, 256 - USB 1.0.

7 Click *Save Policy* to save your changes.

10.7 Data Encryption

The Data Encryption settings determine whether file encryption is enforced on the endpoint device 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.

Encryption is available only on supported releases of Windows XP, Windows Vista*, and Windows 7 (see “Client Requirements” in the *ZENworks Endpoint Security Management 4.1 Installation Guide*. The encryption portion of the security policy is ignored on devices that do not meet the requirement.

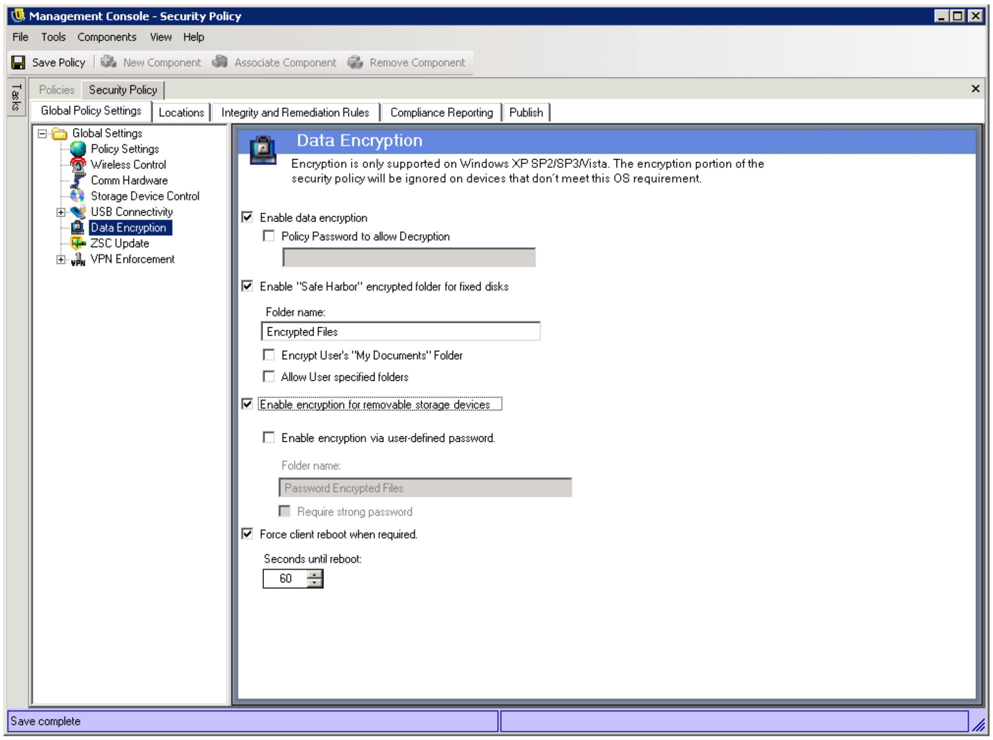
- Section 10.7.1, “Configuring the Data Encryption Settings,” on page 54
- Section 10.7.2, “Data Encryption Performance Impact,” on page 56

WARNING: If you enable encryption on an endpoint device and subsequently want to disable it, make sure that all data stored in encrypted folders is extracted by the user and stored in another location before you disable encryption. In addition, you should export the encryption keys in case any orphaned encrypted files remain; the encryption keys can be used with the decryption utility to decrypt the files. For help exporting the encryption keys, see Section 7.1, “Exporting Encryption Keys,” on page 33. For help using the decryption utility, see Chapter 24, “ZENworks File Decryption Utility,” on page 163.

10.7.1 Configuring the Data Encryption Settings

1 Make sure the policy you want to configure is open in the Management Console (see Section 10.1, “Accessing the Global Settings,” on page 41).

2 On the *Global Policy Settings* tab, click *Data Encryption*.



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

3 Configure the settings as desired:

- **Enable Data Encryption:** Select this option to enable data encryption on a device.

Encryption keys are distributed to all machines that receive security policies regardless of whether data encryption is enabled or not. However, this option instructs the Security Client to activate its encryption drivers, which allows users to read files sent to them without requiring the File Decryption utility. See Section 24, "ZENworks File Decryption Utility," on page 163 for more details.

  - **Policy password to allow decryption:** Specify a password if you want to require users to enter the password prior to decrypting any encrypted files stored in their Safe Harbor folders. This is an optional setting. Leave it blank to not require the password.

- **Enable "Safe Harbor" encrypted folder for fixed disks:** Generates a folder, named `Encryption Protected Files`, at the root of all volumes on the endpoint. All files placed in this folder are encrypted and managed by the 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 specifying the name you want.

  - **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 the authorized user on the machine. If multiple users share the same machine, only the owner of the My Document's folder can access the folder's documents.
  - **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 or network drives can be encrypted.

- **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 can not read the files encrypted on the drive, and can only 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 is 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 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 24, "ZENworks File Decryption Utility," on page 163.

    For example, assume that John is working on encrypted files at work. He wants to take the files home to work on them, but the home computer does not have the Security Client installed. John copies the files to the Password Encrypted Files folder on a USB thumb drive, takes the files home, then accesses them through 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?

- **Force client reboot when required:** On Windows XP, the endpoint must reboot to enable encryption and then reboot a second time to place designated safe harbors into encryption. Any subsequent changes to the safe harbors (adding or removing) also require a reboot. On Windows Vista and Windows 7, no reboots are required.

  Select this option to force the required reboots 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.

4 Click *Save Policy* to save your changes.

10.7.2 Data Encryption Performance Impact

Encrypting and decrypting data on a fixed disk or removable storage device adds additional time to standard file operations such as saving and copying. For example, users can expect the following operations to require more time with encryption enabled:

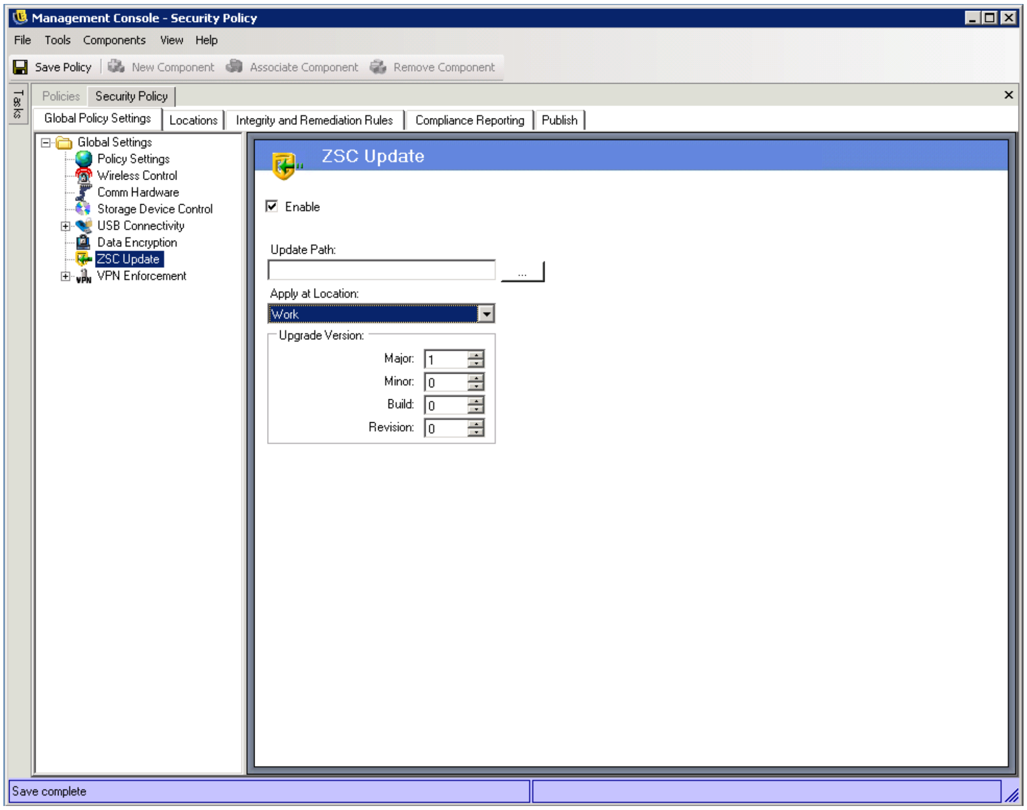
- Copying files or folders to an encrypted removable storage device.
- Saving files from an application to an encrypted removable storage device.
- Copying files or folders from an encrypted removable storage device to a safe harbor on a fixed disk (and vice-versa).

10.8 ZSC Update

Patches to repair any minor defects in the 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 you to specify a location that distributes update patches to end users when they associate to that location.

1 Make sure the policy you want to configure is open in the Management Console (see Section 10.1, “Accessing the Global Settings,” on page 41).

2 On the *Global Policy Settings* tab, click *ZSC Update*.



ZSC Update

☑ Enable

Update Path:

Apply at Location: Work

Upgrade Version:

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

Save complete

3 Check *Enable* to activate update settings.

4 Specify the location where the Security Client looks for the updates.

Because of the file location requirement s in Step 5, you should use the location associated with the enterprise environment (that is, the Work location).

5 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 Security Client, or an MSI file created from the `setup.exe` file. For security purposes, these files should be stored on a secure server behind the corporate firewall.

6 Enter the version information for this file in the provided fields.

Version information is found by installing the Security Client and opening the About screen (see the *ZENworks Endpoint Security Management 4.1 Installation Guide* for details). The version number for `STEngine.exe` is the version number you need to use in the fields.

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

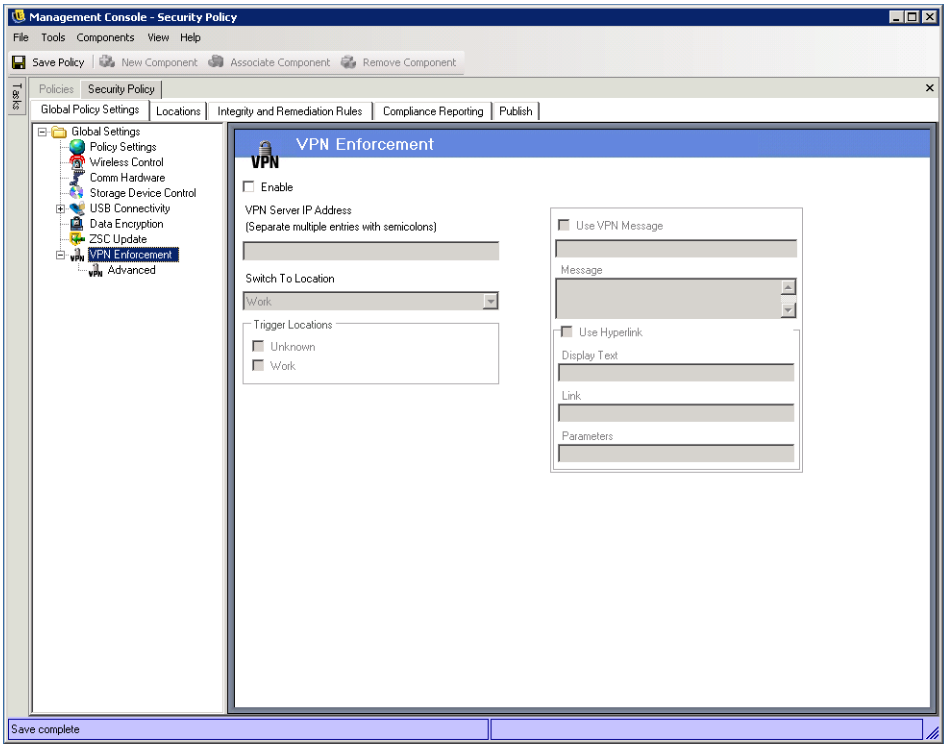
10.9 VPN Enforcement

The VPN Enforcement settings enforce the use of either an SSL or a client-based VPN. VPN enforcement is typically applied at wireless hotspots, allowing the user to associate and connect to the public network, at which time the VPN connection is attempted and the user switched 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 to be connected to a network prior to launching.

NOTE: ZENworks Endpoint Security Management does not support Split Tunnel when configuring VPN settings.

1 Make sure the policy you want to configure is open in the Management Console (see Section 10.1, “Accessing the Global Settings,” on page 41).

2 On the *Global Policy Settings* tab, click *VPN Enforcement*.



3 Select *Enable* to activate VPN enforcement.

4 Specify the IP addresses for the VPN server in the provided field.

If multiple addresses are specified, separate each with a semicolon (for example, 10.64.123.5;66.744.82.36).

5 Select the Switch To location from the drop-down list.

The Switch To location is the location the Security Client switches to when the VPN is activated. The location switch occurs before the VPN connection, after the network has authenticated. This location should apply restrictive security and include 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, and the VPN IP address acts as an ACL to the VPN server, and permits network connectivity.

6 Select the Trigger locations where the VPN enforcement rule is applied.

For strict VPN enforcement, the default Unknown location should be one of the trigger locations. After the network has authenticated, the VPN rule activates and switches to the assigned Switch To location.

7 Specify a Custom User Message to display when the VPN has authenticated to the network.

For non-client VPNs, the message should be sufficient. For VPNs with a client, include a hyperlink that points to the VPN client.

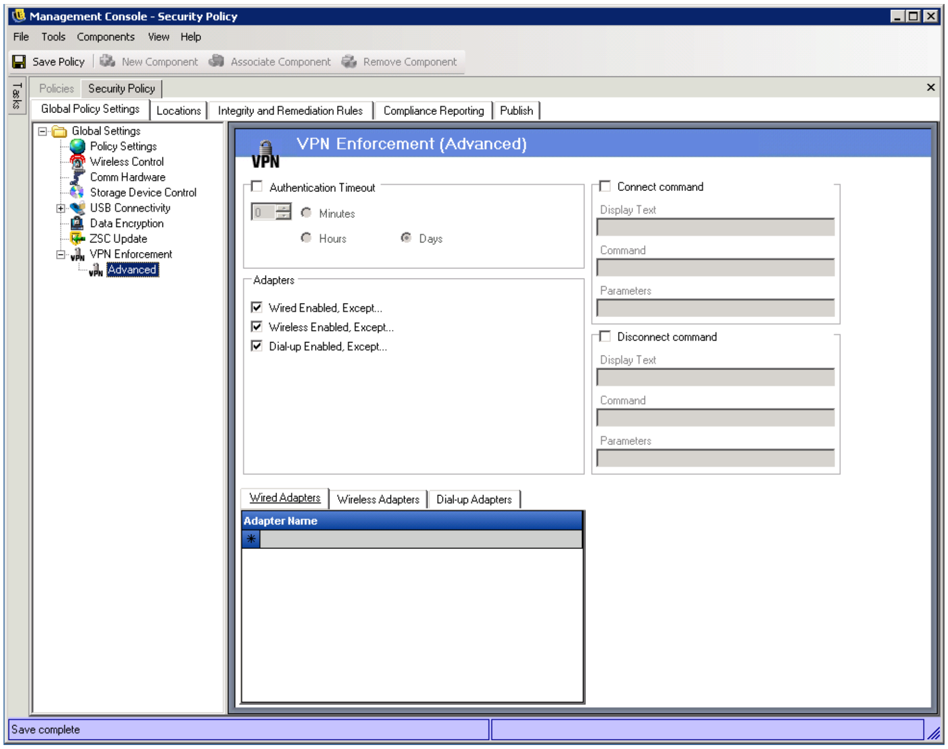
Example: `C:\Program Files\Cisco Systems\VPN Client\ipsecdialer.exe`

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).

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 Security Client is simply comparing the virtual adapter to any adapter restrictions in the current policy.

8 For stricter enforcement, click the "+" symbol next to *VPN Enforcement*, then click *Advanced*.

The standard VPN Enforcement settings you defined make VPN connectivity an option. Users are granted connectivity to the current network whether they launch their VPN or not. The Advance VPN settings 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.



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

9 Configure the settings as desired:

- **Authentication Timeout:** You 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 Security Client waits to gain authentication to the VPN server. You should set this parameter 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 the user to disconnect before logging out of the network.

  VPN clients that generate virtual adapters (for example, Cisco Systems VPN Client 4.0) display the `Policy Has Been Updated` message, and might temporarily switch away from the current location. The Policy has not actually been updated; the Security Client is simply comparing the virtual adapter to any adapter restrictions in the current policy. When running VPN clients of this type the Disconnect command hyperlink should not be used.

- **Adapters:** Select the adapters (Wired, Wireless, Dial-Up) that should have connectivity to the VPN. The *Wired Adapters*, *Wireless Adapters*, and *Dial-up Adapters* lists are exceptions list. If you enable an adapter (for example, you select *Wired Enabled, Except*), the *Wired Adapters* exception list becomes a blacklist; any adapters you add are prohibited. If you disable an adapter (for example, you deselect *Dial-up Enabled, Except*), the *Dial-up Adapters* exception list becomes a whitelist; any adapters you add are allowed.

  This setting overrides any other adapter settings for the Switch To location.

10 Click *Save Policy* to save your changes.

Configuring a Policy's Locations

11

In addition to the global settings for a security policy (see Chapter 10, "Configuring a Policy's Global Settings," on page 41), you can define location-based settings. Unlike global settings, which are applied regardless of location, location-based settings are applied based on the endpoint device's current network environment.

You can use location-based settings to determine firewall security, wireless availability (including allowed access points, encryption security levels, and supported wireless adapters), communication hardware availability (IrDA, Bluetooth, etc.), USB device connectivity, and storage device availability.

- Section 11.1, "Location Concepts," on page 61
- Section 11.2, "Adding a Location," on page 62
- Section 11.3, "Configuring a Location," on page 63

11.1 Location Concepts

You should understand the following concepts before using locations within a policy:

Defined Locations

You define the locations that are appropriate for your organization. When you define a location, you give it a name (for example, Work, Home, or Airport), supply the network environment parameters that identify the location, and configure the security settings to be applied in the location.

For example, you might define a Work location that is identified by specific Gateway servers or wireless access points within your office network. When the Security Client detects those specific network environment parameters, it applies the security settings associated with the Work location.

You can give each location unique security settings, denying access to certain kinds of networking and hardware in more hostile network environments and granting broader access within trusted environments.

The Unknown Location

All policies have an Unknown location that is automatically created with the policy. This is the location the Security Client switches users to when the its current network environment does not match a defined location. You can customize the settings for the Unknown location as needed. For example, you might make the settings more restrictive to provide higher security in the unknown location.

Shared Locations

After you define a location for a policy, the location becomes a shared component that can be used in other policies. For example, you might have one security policy for your corporate office users and another for mobile users. However, you can use the same Corporate Office location in both policies so that mobile users who frequent the corporate office receive the security settings for that location.

If you change the security settings for a shared location, it is changed in all policies. To help ensure that this is acceptable for all policies, you can easily view which policies use a location.

11.2 Adding a Location

There are two ways to add a location. You can define a new location or you can add an existing location.

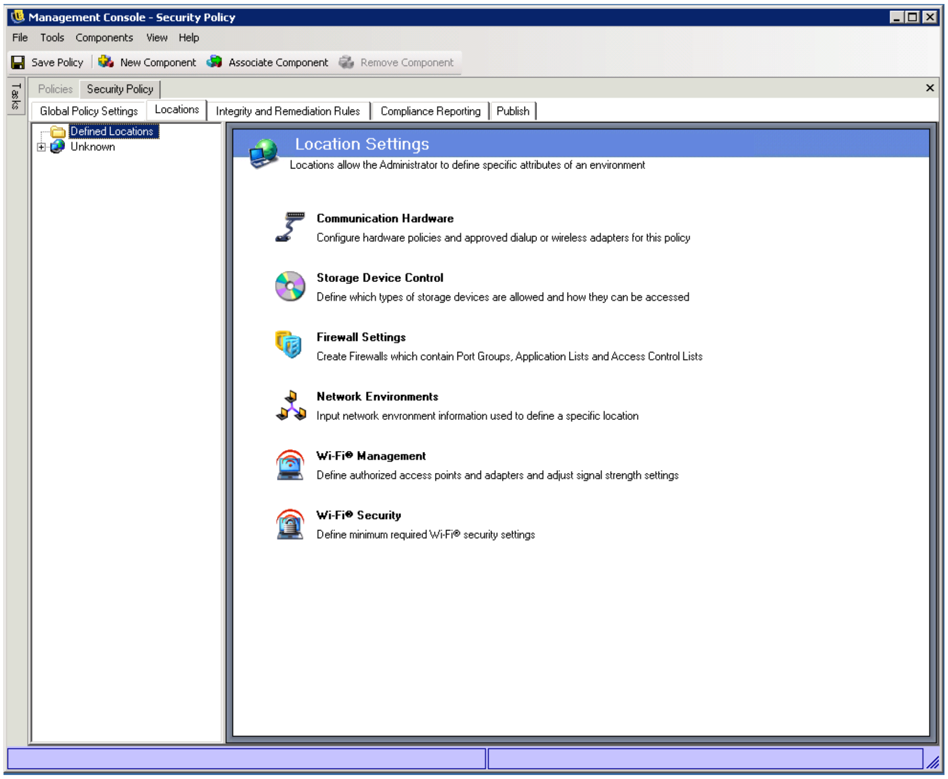
An existing location is one that you defined for another policy; when you define a location for a policy, it is available to share with other policies. Any changes you make in a shared location apply to all policies in which it is used.

Multiple defined locations (beyond simple Work and Unknown locations) can be defined in the policy to provide users with varying security permissions when they connect outside the enterprise firewall.

To add a location to a security policy:

1 In the Management Console, double-click the policy in the *Policies* list.

2 Click the *Locations* tab.



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

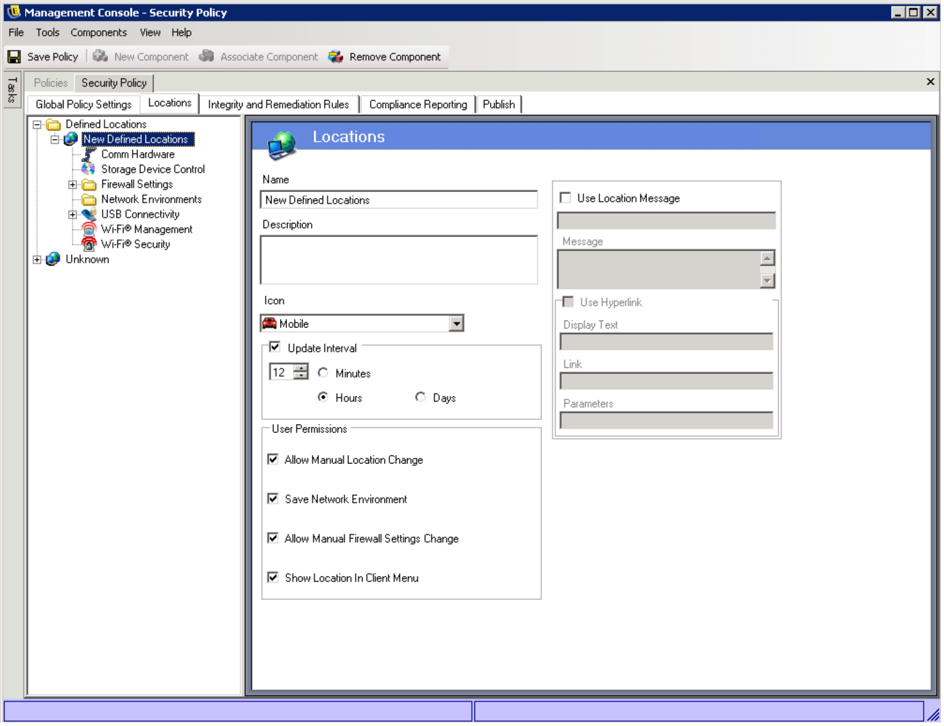
3 In the Locations tree, select *Defined Locations.*

4 If you want to define a new location, click *New Component* on the Policy toolbar.

or

If you want to add an existing location, click *Associate Component* on the Policy toolbar, select the location from the list, then click *OK*.

The location is added under the Defined Locations folder in the Locations tree. If you added a new location, the name is displayed as *New Defined Locations*. If you added an existing location, the location's name is displayed



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

5 Continue with the next section, Configuring a Location.

11.3 Configuring a Location

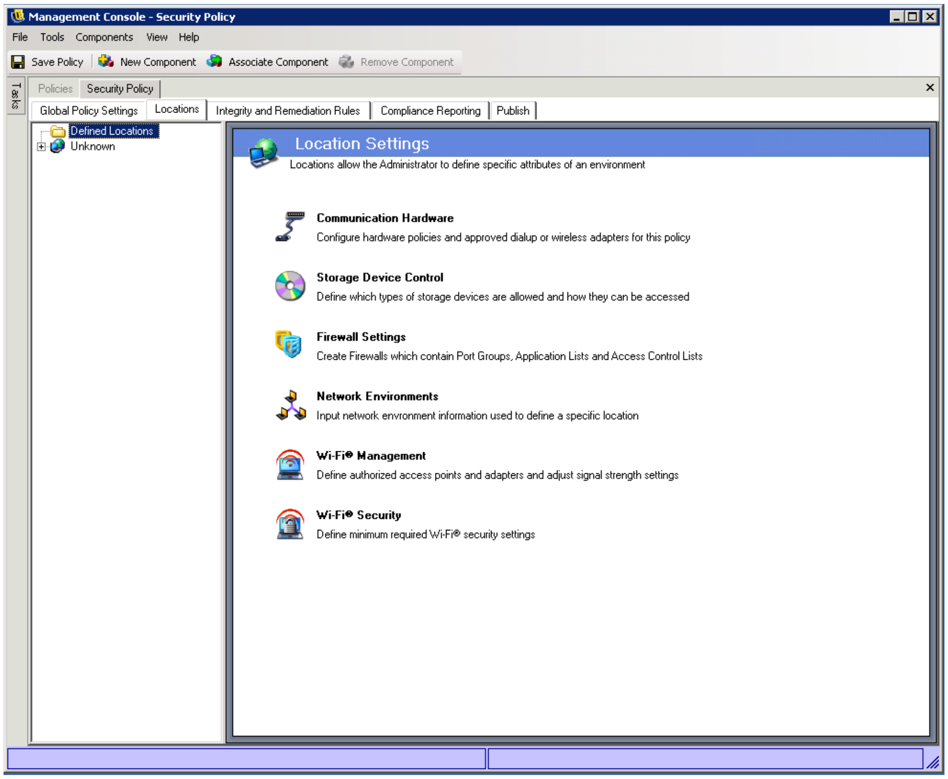
The following instructions help you configure a location's settings, including defining the network environment parameters that identify the location.

Be aware that changing the settings for a location that is shared among policies affects all of the policies. To see if other policies will be affected by the location setting changes, right-click the location name (in the Locations tree), then click *Show Usage*.

1 If the policy's *Location* tab is already displayed in the Management Console, skip to Step 2. Otherwise, open the policy:

1a Double-click the policy in the *Policies* list.

1b Click the *Locations* tab.



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

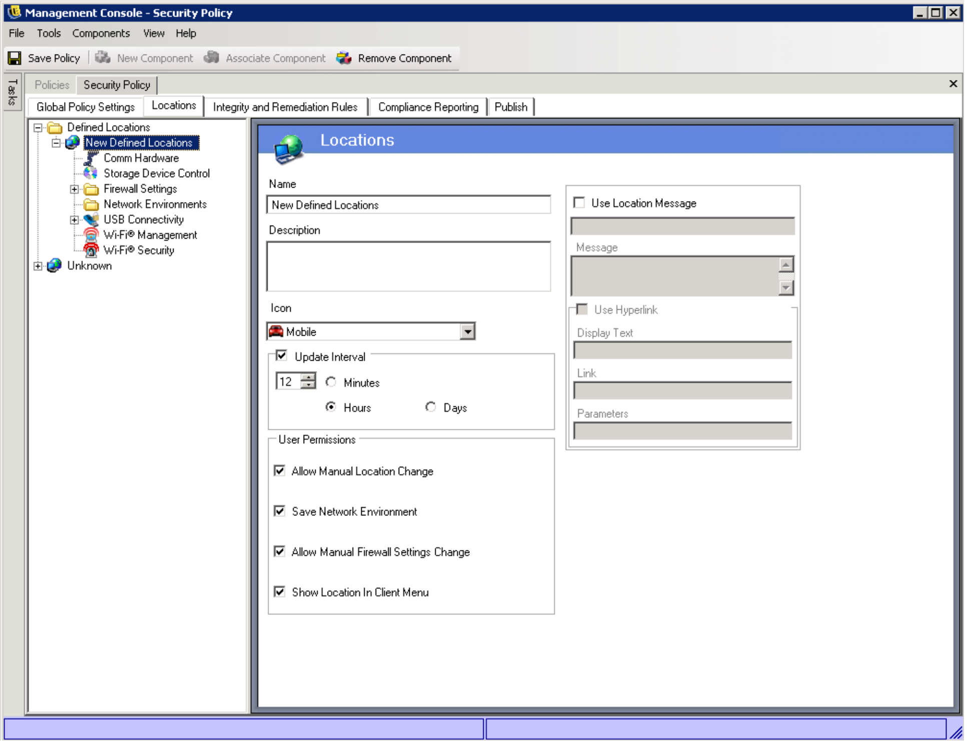
Firewall Settings
Create Firewalls which contain Port Groups, Application Lists and Access Control Lists

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

2 In the Locations tree, select the location whose settings you want to configure.



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:

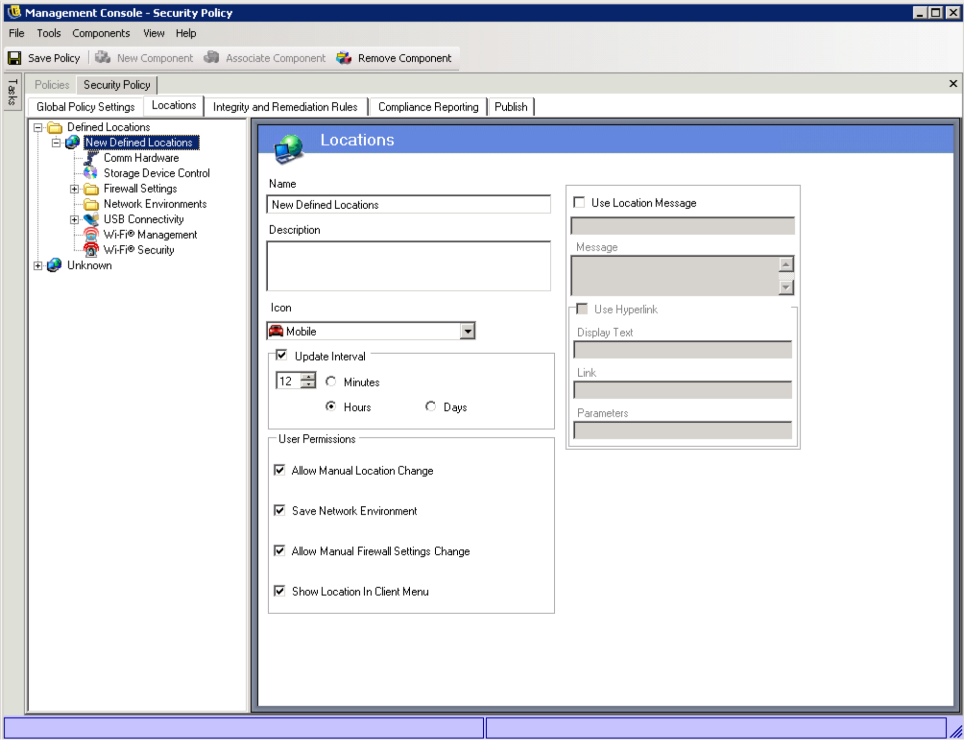
3 Configure the desired location settings by referring to the following sections:

- Section 11.3.1, “Locations,” on page 65
- Section 11.3.2, “Communication Hardware,” on page 66
- Section 11.3.3, “Storage Device Control,” on page 68
- Section 11.3.4, “Firewall Settings,” on page 69
- Section 11.3.5, “Network Environments,” on page 76
- Section 11.3.7, “Wi-Fi Management,” on page 82
- Section 11.3.8, “Wi-Fi Security,” on page 86

11.3.1 Locations

The Locations page lets you name the location, specify how often the Security Client checks for policy updates when associated with the location, and set user permissions for the location.

1 In the Locations tree of the Management Console, select the location.



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 Configure the settings as desired:

- **Name:** Provide a unique name for the location. The name should be easily recognizable to Security Client users.
- **Description:** Provide a description for 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 list to view and select from the available location icons.

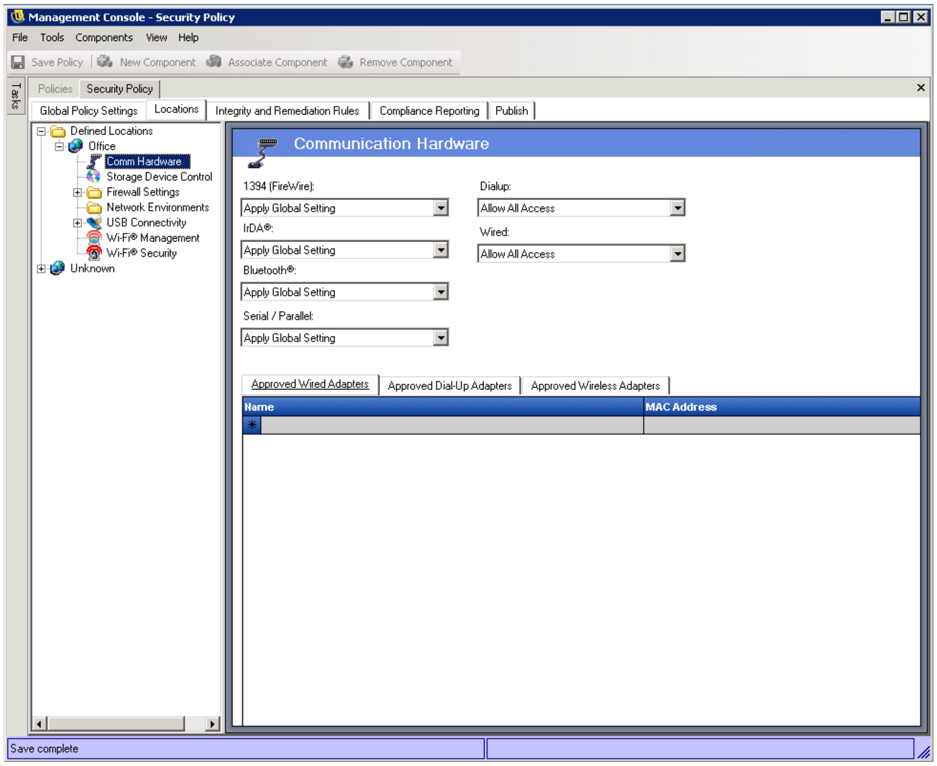
- **Update Interval:** This setting determines how often the Security Client checks for a policy update when it enters this location. The frequency time is set in minutes, hours, or days. Deselecting this parameter means the Security Client does not check for an update at this location.
- **User Permissions:** The following settings determine what the user is allowed to do within the location:
  - **Allow Manual Location Change:** Permits the end user to change to and from this location. For non-managed locations (such as hot-spots, airports, and hotels), this permission should be granted. In controlled environments, where the network parameters are known, this permission can be disabled. The user cannot switch to or from any locations when this permission is disabled. Instead, the location the Security Client chooses (based on the network environment) is the one that is applied.
  - **Save Network Environment:** 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 might need to switch to. Multiple network environments can 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 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.
  - **Allow Manual Firewall Settings Change:** Allows a user to switch from one firewall setting to another.
  - **Show Location in Client Menu:** Displays the location in the Security Client menu. If this is not selected, the location is never displayed.
- **Use Location Message:** Allows an optional Custom User Message to display when the 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.

11.3.2 Communication Hardware

The Communication Hardware settings control which hardware types are permitted a connection at the location.

The Communication Hardware settings are also available as global policy settings (see Section 10.4, “Communication Hardware,” on page 46). The location settings override the global settings and also provide some additional settings that are not available as global settings.

1 In the Locations tree of the Management Console, click the + sign next to the location to expand the location settings, then select *Comm Hardware*.



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

2 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 for the location. 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. If you want to limit access to specific wired adapters, set this option to *All Access* and then add the approved adapters to the *Approved Wired Adapters* list.

3 (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.

4 (Optional) If you have enabled Wi-Fi (see "Wi-Fi Management" on page 82) 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 82), the 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.

5 Click *Save Policy* to save the changes.

The 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.

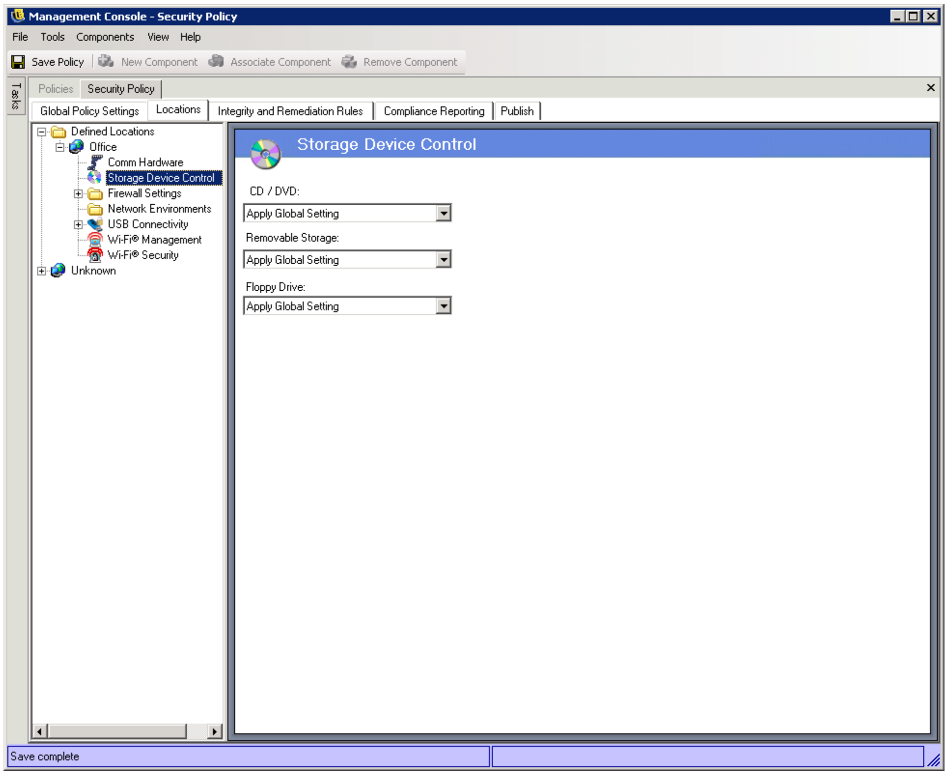
When a new unapproved adapter first installs its drivers on the endpoint (via PCMCIA or USB), the adapter displays as Enabled in Windows Device Manager until the system is rebooted, but all network connectivity is blocked.

11.3.3 Storage Device Control

The Storage Device Control settings determine access to external storage devices (CD/DVDs, removable storage devices, and floppy drives). You can allow read/write access, read-only access, or no access. When a storage device is disabled (no access), users cannot to retrieve any data from the device; however, the hard drive and all network drives remain accessible and operational.

The Storage Device Control settings are also available as global policy settings (see Section 10.4, "Communication Hardware," on page 46). The location settings override the global settings. Some of the global settings, such as *Preferred Devices* and *AutoPlay*, cannot be configured for a location; in this case, the global settings apply to the location.

1 In the Locations tree of the Management Console, click the + sign next to the location to expand the location settings, then select *Storage Device Control*.



Storage Device Control

CD / DVD: Apply Global Setting

Removable Storage: Apply Global Setting

Floppy Drive: Apply Global Setting

Save complete

2 For *CD/DVD*, *Removable Storage*, and *Floppy Drive*, select one of the following options:

- **Apply Global Setting:** Use the global Storage Device Control setting.
- **Allow All Access:** Read/write access is allowed.
- **Disable All Access:** All access is prevented. 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, indicating that the action has failed
- **Read-Only Access:** Read-only access is allowed. 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, indicating that the action has failed

CD/DVD controls all devices listed under *DVD/CD-ROM drives* in Windows Device Manager. *Removable Storage* controls all devices listed under *Floppy disk drives* in Windows Device Manager. *Floppy Drive* controls all devices listed under *Floppy disk drives* in Windows Device Manager.

To disable CD-ROM drives or floppy drives or to set them as read-only, the endpoint device's Local Security Settings 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*. By default, these settings are disabled. If you need to disable them or verify that they are disabled, open either the Active Directory group policy object or open *Administrative Tools* on the target devices. Look in *Local Security Settings - Security Options* and verify that both settings are disabled.

11.3.4 Firewall Settings

Each location is created with a default firewall setting. This default setting, named *All Open*, opens all network ports (all network traffic is allowed), permits all packet types, and allows network access for all applications.

You cannot modify the *All Open* firewall setting. If the location requires a more restrictive firewall setting, you can create a new firewall setting that provides the appropriate protection and designate the new firewall as the default firewall.

You can add multiple firewall settings if necessary. If you add more than one firewall setting, one is defined as the default setting, and the remaining settings are available as options for the user to switch to (if you have allowed firewall switching). Having multiple settings is useful when a user normally needs certain security restrictions within a location and might occasionally need those restrictions either lifted or increased for a short time or for specific types of networking such as ICMP Broadcasts.

To add a firewall setting:

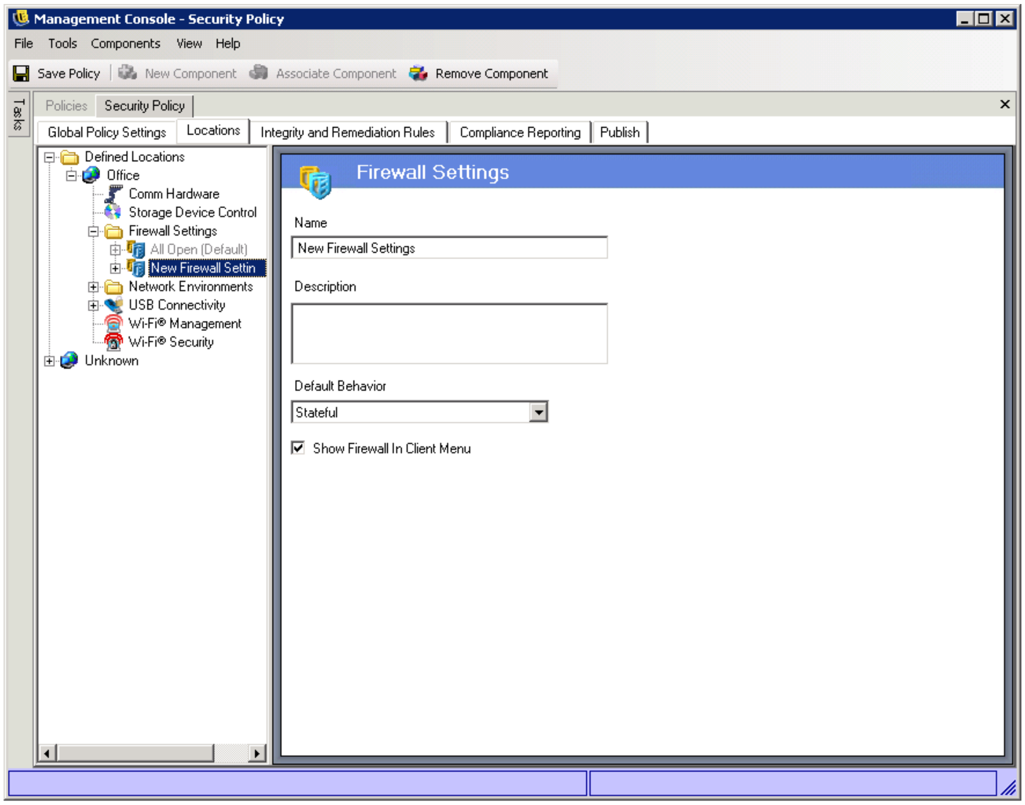
1 In the Locations tree of the Management Console, click the + symbol next to the location to expand the location settings, then select *Firewall Settings*.

2 If you want to define a new firewall setting, click *New Component* on the Policy toolbar.

or

If you want to add an existing firewall setting, click *Associate Component* on the Policy toolbar.

The firewall setting is added under the Firewall Settings folder in the Locations tree. If you add a new firewall setting, the name is displayed as *New Firewall Settings*. If you add an existing firewall setting, the setting's name is displayed



Name: New Firewall Settings

Description:

Default Behavior: Stateful

☑ Show Firewall In Client Menu

3 On the Firewall Settings page, fill in the following fields:

- **Name:** Specify a name for the firewall setting
- **Description:** Specify a description.
- **Default Behavior:** Select the default behavior for the TCP/UDP ports:
  - **Open:** All network inbound and outbound traffic is allowed.
  - **Closed:** All inbound and outbound network traffic is blocked.
  - **Stateful:** All unsolicited inbound network traffic is blocked. All outbound network traffic is allowed.

    Please note that the *Stateful* setting does not allow an active FTP session; you must use passive FTP instead. A good reference to explain active versus passive FTP is the Slacksite Web site (http://slacksite.com/other/ftp.html).

  You can use the TCP/UDP Ports page and the Access Control Lists page to override these default settings for specific ports and protocols.

  For example, assume that 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.

- **Show Firewall in Client Menu:** Select this option to have the firewall displayed in the Security Client menu. This is necessary only if the user is allowed to switch firewalls for a location (see User Permissions).

4 If you want this firewall setting to be the default for this location, right-click the firewall setting in the Location tree, then click *Set as Default*.

5 Click *Save Policy* to save your changes.

6 Configure the desired firewall settings by referring to the following sections:.

- "TCP/UDP Ports" on page 71
- "Access Control Lists" on page 73
- "Application Controls" on page 74

TCP/UDP Ports

The TCP/UDP Ports setting allows you to create a TCP/UDP port group and assign a behavior (Open, Closed, or Stateful) to the group. The behavior overrides the default port behavior configured for the firewall setting (see Step 3 on page 70).

Be aware that when enforcing the firewall settings, the Security Client does not allow incoming connections to dynamically assigned ports. If an application requires an incoming connection, the port must be static and included in a TCP/UDP port group that is assigned the Open behavior. If the incoming connection is from a known remote device, an Access Control List can be used.

To add a new TCP/UDP port group:

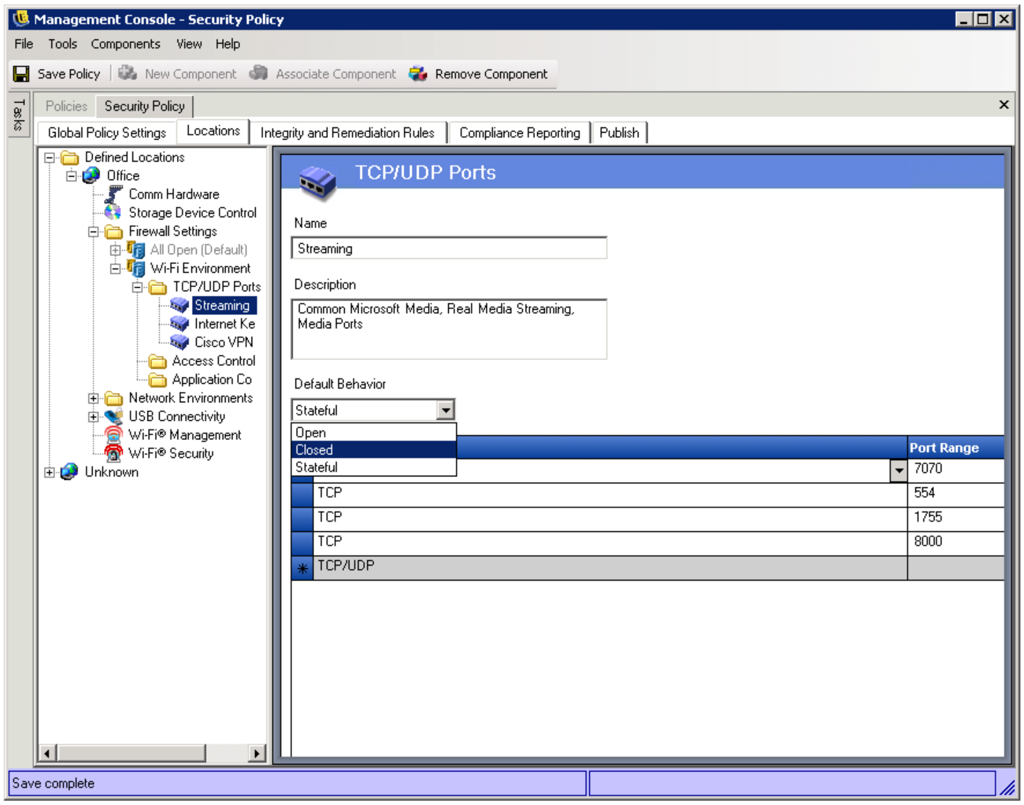
1 In the Locations tree of the Management Console, select the *TCP/UDP Ports* folder (*Defined Locations* > *location* > *Firewall Settings* > *firewall* > *TCP/UDP Ports*).

2 If you want to define a new TCP/UDP port group, click *New Component* on the Policy toolbar.

or

If you want to add an existing TCP/UDP port group, click *Associate Component* on the Policy toolbar. For information about the predefined port groups that you can use, see Appendix A, "Predefined TCP/UDP Port Groups," on page 171.

The port group is added under the TCP/UDP Ports folder in the Locations tree. If you add a new port list, the name is displayed as *New TCP/UDP Ports*. If you add an existing port list, the port list's name is displayed



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	

3 On the TCP/UDP Ports page, fill in the following fields:

- **Name:** Specify a name for the port group.
- **Description:** Specify a description.
- **Default Behavior:** Select the behavior to apply to the port group:
  - **Open:** All inbound and outbound network traffic is allowed.
  - **Closed:** All inbound and outbound network traffic is blocked.
  - **Stateful** - All unsolicited inbound network traffic is blocked. All outbound network traffic is allowed.

4 Add ports to the group:

4a Click the *Port Type* field to select the port type (*TCP/UDP*, *Ether*, *IP*, *TCP*, or *UDP*).

4b In the *Port Range* field, specify a single port or a range of ports:

For example, 1-100 would add all ports between 1 and 100.

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

4c Repeat Step 4a and Step 4b to add additional ports to the group.

If you need to delete a port, select the port's row, press the *Delete* key on the keyboard, and click *Yes* to confirm the deletion.

5 Click *Save Policy* to save your changes.

Access Control Lists

Some IP or MAC addresses might require unsolicited traffic to be passed regardless of the current port behavior (such as an enterprise back-up server or exchange server). In instances where unsolicited traffic needs to be passed to and from trusted servers, an Access Control List (ACL) can be created to provide this support.

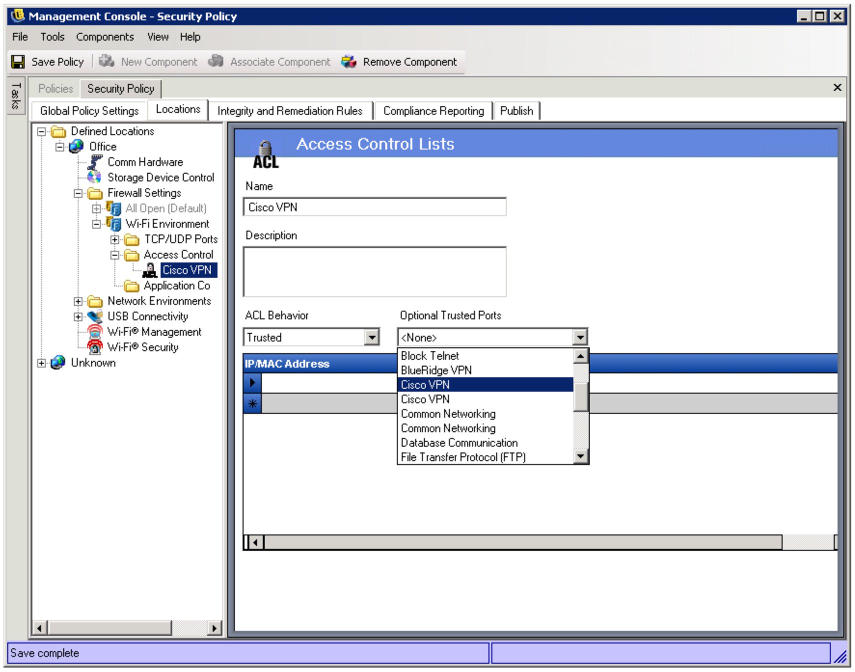
To add an Access Control List:

1. In the Locations tree of the Management Console, select the Access Control Lists folder (*Defined Locations > location > Firewall Settings > firewall > Access Control Lists*)
2. If you want to define a new list, click *New Component* on the Policy toolbar.

   or

   If you want to add an existing list, click *Associate Component* on the Policy toolbar. For information about the predefined lists that you can use, see Appendix B, "Predefined Access Control Lists," on page 173.

   The Access Control List is added under the Access Control Lists folder in the Locations tree. If you add a new list, the name is displayed as *New Access Control Lists*. If you add an existing list, the list's name is displayed



Name: Cisco VPN

Description:

ACL Behavior: Trusted

Optional Trusted Ports: <None>

3. Name the ACL and provide a description.
4. Add addresses to the list. To do so:

   4a In the IP/MAC Address field, specify the address:

   - **IP:** Specify a single standard IP address (example: 123.45.6.189) or a range of IP addresses (example: 123.0.0.0 - 123.0.0.255).
   - **MAC:** Specify a standard MAC address separated by colons (example: 00:01:02:34:05:B6).

- **ACL Macro:** There are 16 predefined ACLs that you can add to the list. For information about using the ACLs, see Appendix B, “Predefined Access Control Lists,” on page 173.

4b Click the Type field to select the address type (*IP* or *MAC*).

4c Repeat Step 4a and Step 4b to add additional addresses to the list.

If you need to delete an address, select the row, press the *Delete* key on the keyboard, and click *Yes* to confirm the deletion.

5 In the *ACL Behavior* list, select whether the ACL is *Trusted* (allow it always even if all TCP/UDP ports are closed) or *Non-Trusted* (access is blocked).

6 If the ACL Behavior is *Trusted*, select the Optional Trusted Ports (TCP/UDP) for this ACL to use.

These ports permit all ACL traffic, while other TCP/UDP ports maintain their current settings. Selecting *‹None›* means any port may be used by this ACL.

7 Click *Save Policy* to save your changes.

Application Controls

The *Application Controls* setting lets you block applications either from executing or from gaining network access.

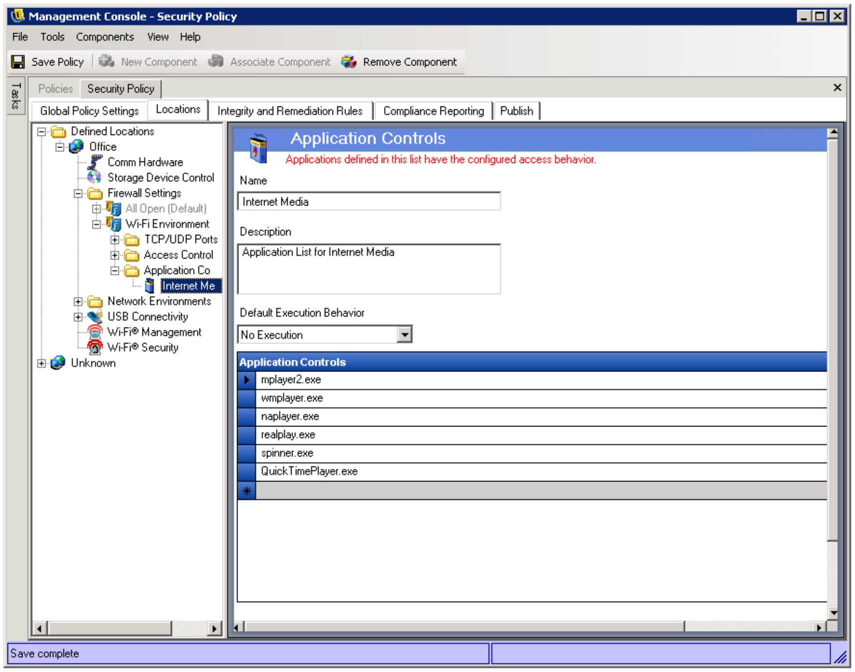
1 In the Locations tree of the Management Console, select the Application Controls folder (*Defined Locations* > *location* > *Firewall Settings* > *firewall* > *Application Controls*)

2 If you want to define a new control, click *New Component* on the Policy toolbar.

or

If you want to add an existing control, click *Associate Component* on the Policy toolbar.

The Application Control is added under the Application Controls folder in the Locations tree. If you added a new list, the name is displayed as *New Application Controls*. If you added an existing control, the control’s name is displayed



Application Controls

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

3 Name the application control and provide a description.

4 Select an execution behavior.

This behavior is applied to all applications listed. If multiple behaviors are required (for example, some networking applications are denied network access, but all file sharing applications are denied execution), you need to define multiple application controls. Select one of the following:

- **No Execution:** All applications listed are not permitted to execute.
- **No Internet Access:** All applications listed are denied Internet access. Applications (such as Web browsers) launched from an application will also be denied access.

Be aware of the following:

- Application Control does not function if the endpoint device is booted to Safe Mode with Networking.
- Blocking execution of an application does not shut down the application if it is already open on the endpoint device.
- Blocking execution of an application does not stop the application if it is started from a network share that has System blocked from read access.
- Blocking Internet access for an application does not affect saving files to mapped network drives. Users are permitted to save to all network drives available to them.
- Blocking Internet access for an application does not stop the application if it is already actively streaming network data to the endpoint device.
- Blocking Internet access for an application does not stop the application from getting data from a network share.

5 Add applications to the list by using the following guidelines:

- Add one application per row.
- Specify only the executable name (no path).

- If you need to delete an application, select the row, press the *Delete* key on the keyboard, and click *Yes* to confirm the deletion.
- If the same application is added to two different Application Controls in the same firewall setting (for example, `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).

IMPORTANT: Blocking execution of critical applications could have an adverse affect on system operation. Blocked Microsoft Office applications will attempt to run their installation program.

6 Click *Save Policy* to save your changes.

11.3.5 Network Environments

The *Network Environments* settings let you specify the network services (Gateway servers, DNS servers, wireless access points, and so forth) that identify the location. You can specify which services are required and which are optional. For the device's current environment to match the defined network environment and associate the device to the network environment's location, required services must be present and optional services might or might not be present.

To define a network environment for the location:

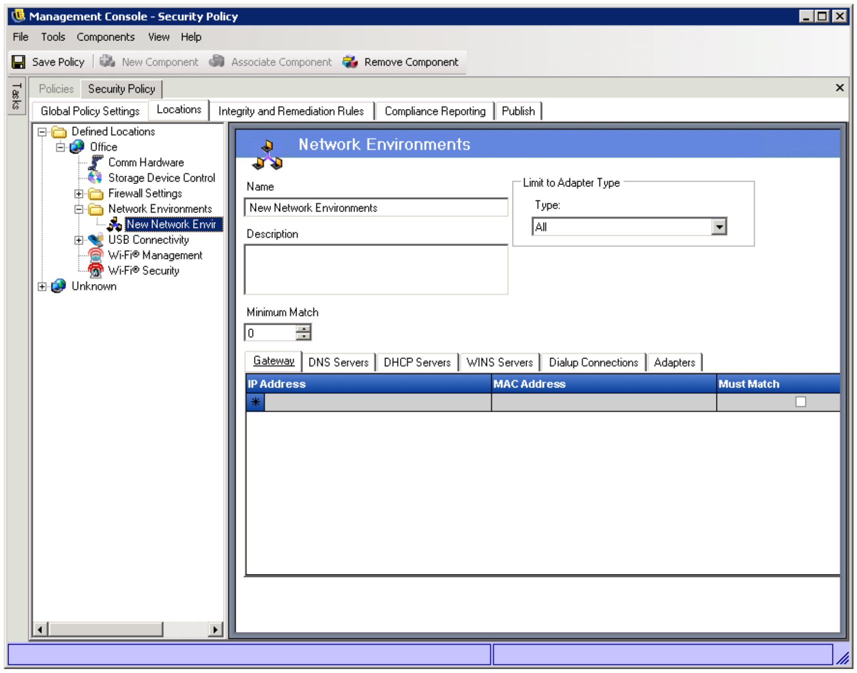
1 In the Locations tree of the Management Console, select the Network Environments folder (*Defined Locations* > *location* > *Network Environments*).

2 If you want to define a new network environment, click *New Component* on the Policy toolbar.

or

If you want to add an existing network environment, click *Associate Component* on the Policy toolbar.

The network environment is added under the Network Environments folder in the Locations tree. If you add a new network environment, the name is displayed as *New Network Environments*. If you add an existing network environment, the environment's name is displayed.


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
Defined Locations
Office
Comm Hardware
Storage Device Control
Firewall Settings
Network Environments
New Network Envir
USB Connectivity
Wi-Fi® Management
Wi-Fi® Security
Unknown
Network Environments
Gateway | DNS Servers | DHCP Servers | WINS Servers | Dialup Connections | Adapters
IP Address | MAC Address | Must Match

Name: New Network Environments

Description:

Limit to Adapter Type — Type: All

Minimum Match: 0

3 Name the network environment and provide a description

4 If you want to limit when this network environment is available based on adapter type, use the *Limit to Adapter Type* field to select the allowed adapter type. The default (*All*) allows all adapter types.

5 For each service (*Gateway*, *DNS Servers*, *DHCP Servers*, and *WINS Server*) you want to use to define the network, specify the following information to define the service:

- **IP Address:** Limited to 15 characters. Use only the numbers 0-9 and periods (for example, 123.45.6.789)
- **MAC Address (Optional):** Limited to 12 characters. Use only the numbers 0-9 and the letters A-F (uppercase and lowercase) separated by colons (for example, 00:01:02:34:05:B6). The *DNS Servers* list does not include this field.
- **Must Match:** Select whether the presence of this service is required to identify the network environment

6 For *Dialup Connection*s, specify the phone book entry:

The RAS Entry name from the phone book or the dialed number can be specified. Phone book entries can contain alphanumeric characters (a-z, 1-9) and special characters (@, #, $,%, -, etc.), but cannot contain only numeric characters and special characters. Entries that only contain special and numeric characters are assumed to be dialed numbers.

7 If you want to restrict the allowed adapters to specific adapters, use the *Adapters* list.

Adapters can be specified to restrict the allowed adapter types (see Step 4) to specific adapters. Enter the SSID for each allowed adapter. If no SSIDs are specified, all adapters of the permitted type are granted access

8 In the *Minimum Match* field, select the minimum number of network services that must match in order for this network environment to match the device's current environment.

This number must be equal to or greater than the number of Must Match services you defined. For example, if you defined four Must Match services and ten optional services, you could specify 7 in the *Minimum Match* field. This would required all four Must Match services to be matched along with any three of the ten optional services.

9 Click *Save Policy* to save your changes.

You can associate additional network environments to the location. 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 causes unpredictable results and is not recommended.

11.3.6 USB Connectivity

The USB Connectivity settings control access to devices that connect via the USB bus. The settings provide control at the following levels: all devices, device groups (classes), and individual devices. This gives you great flexibility in defining approved devices (whitelists) and prohibited devices (blacklists).

For example, assume that your organization supports only two authorized USB printers. You could allow access to all USB devices, block access to the printer device class, and then allow access to your two authorized printers. The result is a printer whitelist that includes only your two authorized printers.

The USB Connectivity settings are also available as global policy settings (see Section 10.6, “USB Connectivity,” on page 49). The location settings override the global settings.

- “How the Access Setting Is Determined” on page 78
- “Configuring the USB Connectivity Settings” on page 79

How the Access Setting Is Determined

To effectively use the USB Connectivity settings, you need to understand how the various settings are used to determine a device’s access.

When a device is detected, the first setting that is evaluated is the *USB Devices* setting. If the *USB Devices* setting is *Allow All Access*, the evaluation continues. If the setting is *Disable All Access*, the USB device is disabled and evaluation stops.

If the evaluation continues, the device’s attributes (Device Class, Manufacturer, Product, and so forth) are compared to the attributes associated with the device groups (in *Device Group Access*) and individual devices (in the device list on the *Advanced* page). In some cases, the device might match more than one group and device. For example, a removable storage device might match both the Mass Storage Class group and an individually defined device.

In order to know which access setting to apply to a USB device, the Security Client builds an access filter against which to evaluate devices. If multiple security policies apply, the Security Client uses the USB Connectivity settings from all applied policies to build the access filter.

The filter includes each access setting (*Always Block*, *Always Allow*, *Block*, *Allow*, and *Default Device Access*) and the device groups and devices assigned to the setting. For example, assume the following group and device assignments for each access setting:

Access Setting	Group Assignments	Device Assignment
Always Block		Mouse1
		Thumbdrive2, Thumbdrive5
Always Allow	Human Interface Device	Printer4, Printer3, Printer1
Block	Printing Class	Scanner1
Allow	Mass Storage Class	Printer2
	Scanning/Imaging (PTP	

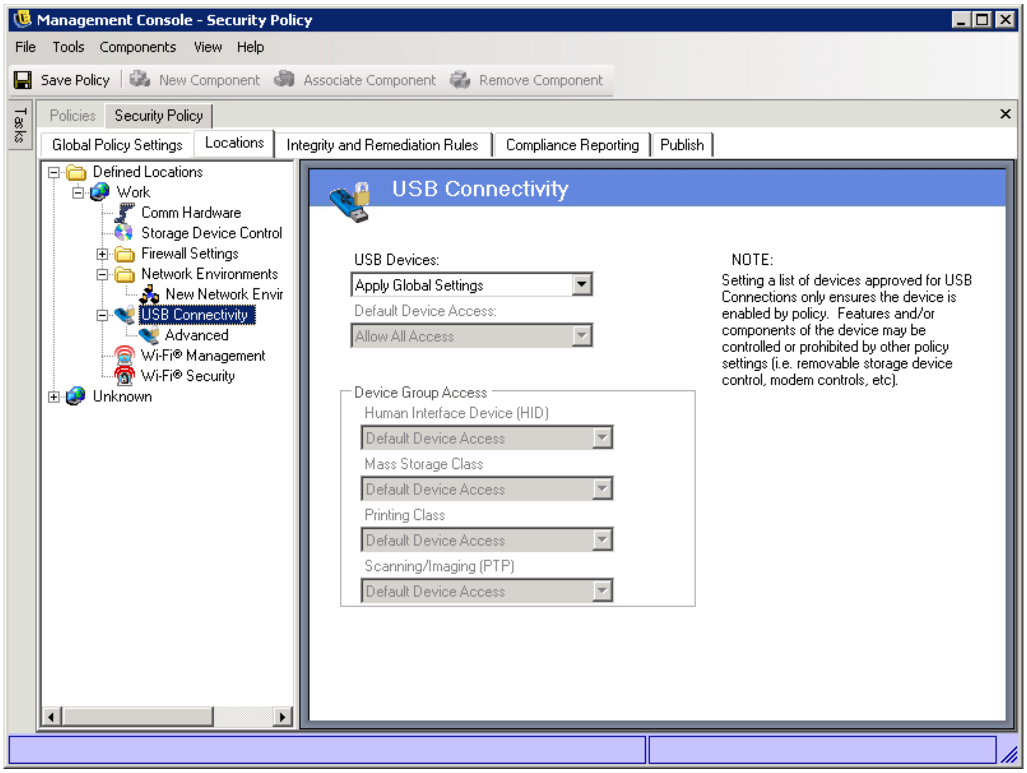
A USB device is evaluated against the filter, beginning with the first setting (*Always Block*) and continuing to the last (*Allow*). If the device matches one of the device groups or devices assigned to the access setting, the device receives that access setting and the evaluation ends. If a device does not match any of the groups or devices, it receives the default device access.

Consider the following examples:

- Mouse1(a Human Interface Device) is detected. It is evaluated against the first setting (*Always Block*). Because Mouse1 matches the Mouse1 device assignment for the *Always Block* setting, Mouse1 is blocked and no further evaluation is required.
- Mouse4 (a Human Interface Device) is detected. It is evaluated against the *Always Block* setting. Mouse4 does not match any *Always Block* assignments (group or device), so it is evaluated against the *Always Allow* assignments. Because Mouse4 is a Human Interface Device and that device group is assigned the *Always Allow* setting, Mouse4 is allowed and no further evaluation is required.
- Thumbdrive1 and Thumbdrive5 (two Mass Storage Class devices) are detected. Thumbdrive5 is blocked because its device assignment (*Always Block*) precedes its Mass Storage Class group assignment (*Allow*). Thumbdrive1 is allowed because it is included in the Mass Storage Class group assignment (*Allow*) and it does not match a device assignment.
- Printer2 and Printer4 (two Printing Class devices) are detected. Printer4 is allowed because its device assignment (*Always Allow*) precedes its Printing Class group assignment (*Block*). Printer2 is blocked because its Printing Class group assignment precedes its device assignment (*Allow*).

Configuring the USB Connectivity Settings

1 In the Locations tree of the Management Console, click the + sign next to the location to expand the location settings, then select *USB Connectivity.*



USB Devices: Apply Global Settings

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).

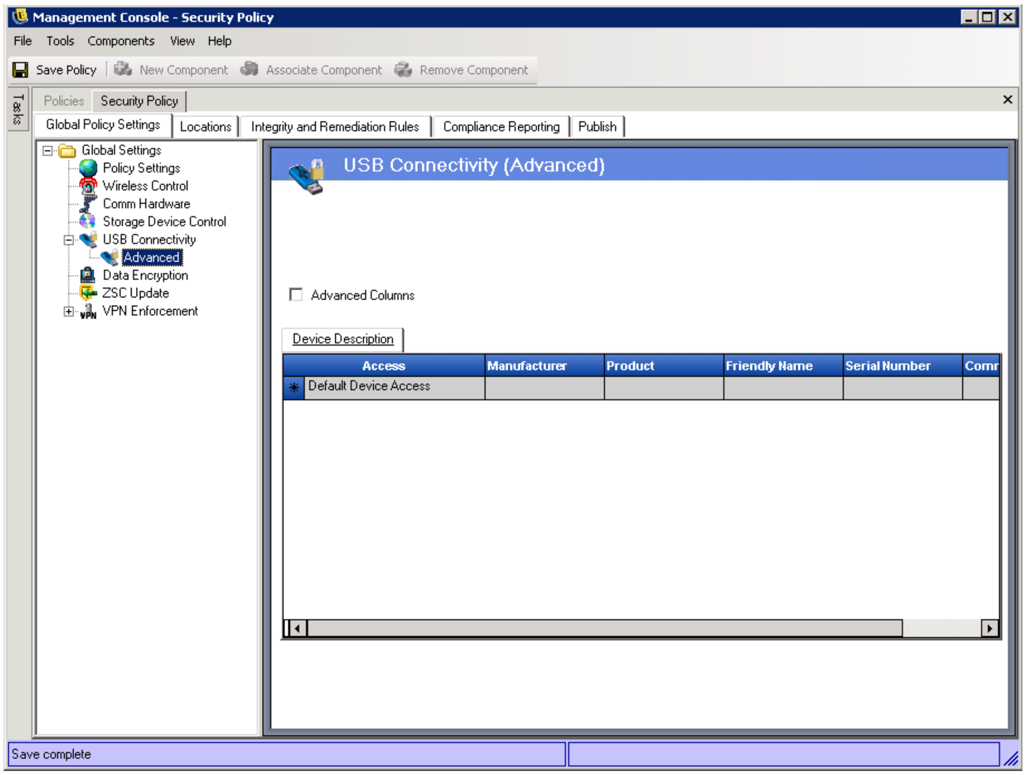
2 Configure the settings as desired:

- **USB Devices:** Device access is first evaluated based on whether the USB bus is active or not. 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 Security Client continues the evaluation based on the remaining settings. Select *Apply Global Settings* if you want to use the policy's global USB Connectivity settings.
- **Default Device Access:** Select the default access (*Allow All Access* or *Disable All Access*) that will be assigned to USB devices in the following situations:
  - A USB device does not match one of the defined device groups or devices.
  - A USB device matches a defined device group or device whose access is set to *Default Device Access*.
- **Device Group Access:** For each device group listed, select the access you want assigned to the group:
  - **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.

The device groups are determined by the following classes. If a USB device's class corresponds to one of the groups, it receives the group's assigned access.

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.

3 If you want to define individual devices, click the plus sign next to *USB Connectivity* in the *Locations* tree, then click *Advanced*. Otherwise, skip to Step 6.



☐ Advanced Columns

Access	Manufacturer	Product	Friendly Name	Serial Number	Comr
Default Device Access					

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.

4 To add a device to the list, fill in the device fields.

A device makes a set of attributes available to the OS. These attributes are matched by the Security 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 that a device provides the following attributes: Manufacturer: Acme, Class: 8, Serial Number: "1234".

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

The *Manufacturer*, *Product*, and *Friendly Name* fields are substring matched. All other fields are exact matches.

- **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* filter 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 (such as Canon). This is a substring match field, meaning that both *C* and *Can* would match *Canon*.
- **Product:** Click the *Product* column, then type the name of the product. This is a substring match field, meaning that both *C* and *Can* would match *Canon*.
- **Friendly Name:** Click the *Friendly Name* column, then type the friendly name of the device. This is a substring match field, meaning that both *C* and *Can* would match *Canon*.
- **Serial Number:** Click the *Serial Number* column, then type the serial number of the device. A serial number produces a unique match only when used with the *USB Version*, *Vendor ID*, *Production ID*, and *BCD Device* fields. This is an exact match field.
- **Comment:** Click the *Comment* column, then type a comment. This field is not used to match devices, so it can include any text you want.

5 If you want to use additional attributes to define the device, click *Advanced Columns*

This adds 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*.

All fields are exact match fields. Current valid values for the USB version in decimal are 512 - USB 2.0, 272 - USB 1.1, 256 - USB 1.0.

6 Click *Save Policy* to save your changes.

11.3.7 Wi-Fi Management

The Wi-Fi Management settings are available only if Wi-Fi transmissions are enabled in the global Wireless Control settings (see Section 10.3, “Wireless Control,” on page 44).

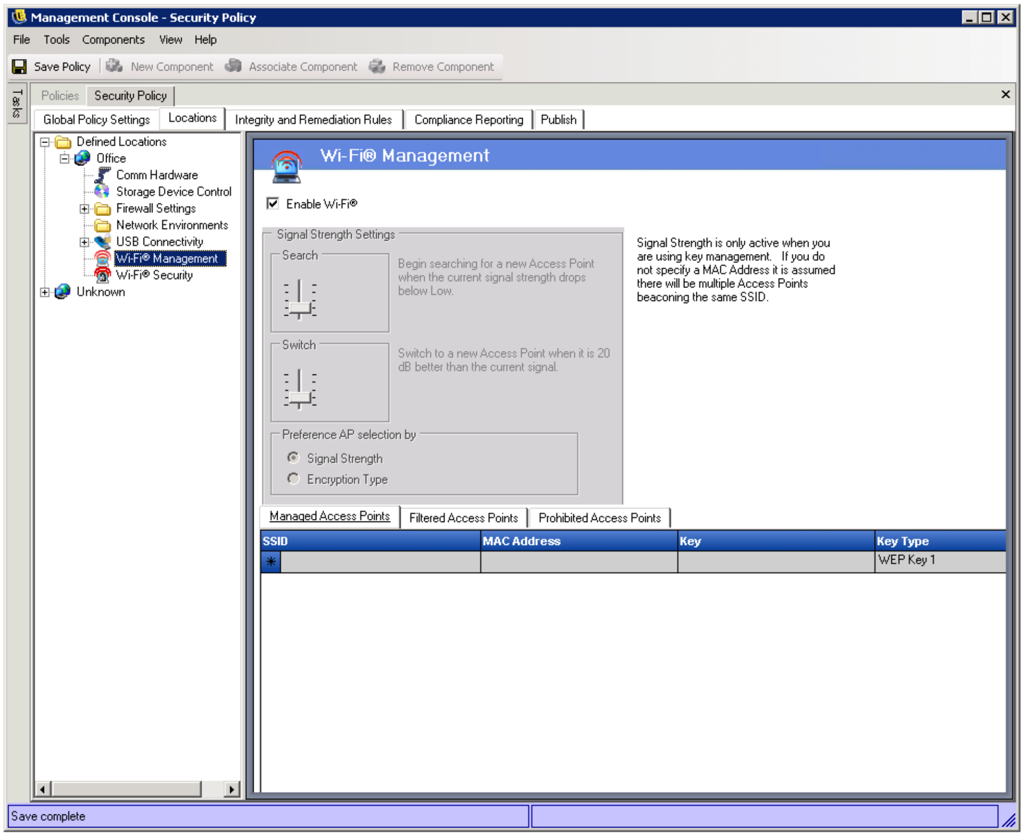
The Wi-Fi Management settings let you do the following:

- Enable or disable Wi-Fi transmissions for the location. If you disable transmissions, all other settings are also disabled.

- Control connections to access points by creating *Managed Access Points*, *Filtered Access Points*, and *Prohibited Access Points* lists.
- For managed access points, set up automatic switching based on access point signal strength and encryption type.

To configure the Wi-Fi Management settings:

1 In the Locations tree of the Management Console, click the + sign next to the location to expand the location settings, then select *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

2 Select *Enable Wi-Fi* to enable wireless transmissions in this location.

This setting enables or disables the endpoint device's wireless adapters. It applies to all supported Security Client operating systems (Windows 2000, XP, Vista, and 7).

3 Add access points to the *Managed Access Points*, *Filtered Access Points*, and *Prohibited Access Points* lists.

The access point lists apply only to Windows XP endpoint devices. The Security Client does not support access point lists on Windows 2000, Vista, or 7 endpoint devices.

The Security Client integrates with the Windows XP Wireless Zero Configuration service to control the access points. The endpoint device should not use any third-party wireless network managers when managing access points through the Security Client. In essence, the Security Client functions as the wireless network manager; using a third-party wireless network manager can interfere with the Security Client and cause unpredictable results.

If an endpoint device is using a third-party wireless network manager, you should either 1) uninstall the manager, 2) prevent the manager from starting (for example, through an application control in the Firewall settings), or 3) instruct the user to delete any preferred network lists from the manager and not use the manager.

- **Managed Access Points:** A managed access point is one for which you automatically distribute and apply Wired Equivalent Privacy (WEP) keys without user intervention. This protects the integrity of the keys by not passing them in the clear.

  Because of the inherent security vulnerabilities of Shared WEP Key Authentication, Novell supports Open WEP Key Authentication only.

  Specify the following information for each managed access point you want to define

  - **SSID:** Specify the SSID number. The SSID number is case sensitive.
  - **MAC Address:** Specify the MAC address. This is recommended because SSIDs might be duplicated. If the MAC address is not specified, it is assumed that 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:** Specify the encryption key index by selecting the appropriate level from the drop-down list.
  - **Beaconing:** Select this option if the defined access point is currently broadcasting its SSID. Leave it deselected if this is a non-beaconing access point.

  The Security Client attempts to first connect to each beaconing access point listed in the policy. If no beaconing access is located, the 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 Step 4).

- **Filtered Access Points:** Specify the access points that can be displayed in the Wireless Zero Configuration interface. This only affects the access points that are displayed to users. Users can still connect to a non-displayed access point by manually entering the information. To prevent a user from connecting to an access point, you must add it to the *Prohibited Access Points* list.

  Specify the following information for each access point:

  - **SSID:** Specify the SSID number. The SSID number is case sensitive.
  - **MAC Address:** Specify the MAC address. This is recommended because SSIDs might be duplicated. If the MAC address is not specified, it is assumed that there are multiple access points beaconing the same SSID number.

- **Prohibited Access Points:** Access points in the *Prohibited Access Points* list do not display in the Wireless Zero Configuration interface, nor can the endpoint device connect to them.

  Specify the following information for each access point you want to prohibit:

  - **SSID:** Specify the SSID number. The SSID number is case sensitive.
  - **MAC Address:** Specify the MAC address. This is recommended because SSIDs might be duplicated. If the MAC address is not specified, it is assumed that there are multiple access points beaconing the same SSID number.

4 Configure the *Signal Strength* settings.

When more than one WEP-managed access point is defined in the *Managed Access Points* list, 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 Security Client searches for, discards, and switches to another access point defined in the list.

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

- **Search:** When this signal strength level is reached, the 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 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. Because each Wi-Fi card and radio might 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. You should research your Wi-Fi adapter's RSSI values to supply 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

These signal strength names match those used by the Microsoft Zero Configuration Service, but the thresholds might 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 receives a signal at -54 dB and has a noise level of -22 dB, the SNR reports as 32dB (-54 - -22=32), which on the Zero Configuration scale translates as Excellent signal strength. However, on the Novell scale, the -54 dB signal indicates a Very Good signal strength.

The end user never sees the Novell signal strength thresholds; this information is provided to show the difference between what the user might see through Zero Config and what is actually occurring in the Security Client.

Because both signal strength and encryption type (see "Wi-Fi Security" on page 86) 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, the strongest signal is given preference when connecting. If WEP 64 is the encryption requirement and encryption is the preference, access points with the highest encryption strength are given preference over all others.

5 Click *Save Policy* to save your changes.

11.3.8 Wi-Fi Security

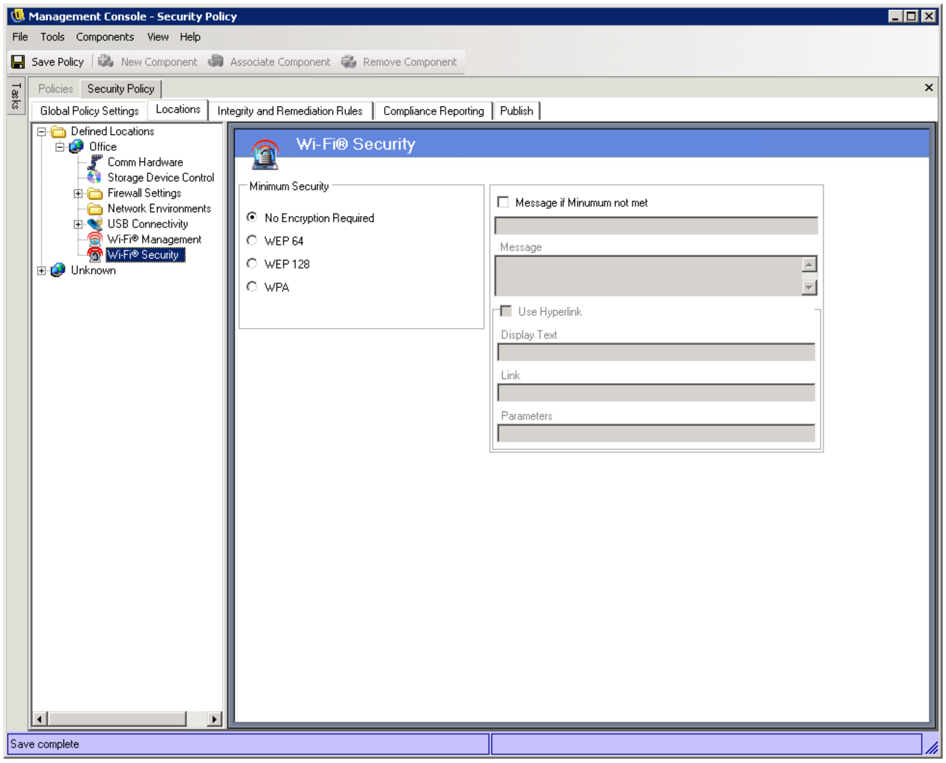
The Wi-Fi Security settings are available only if Wi-Fi transmissions are enabled in the global Wireless Control settings (see Section 10.3, “Wireless Control,” on page 44) and in the location’s Wi-Fi Management settings (see Section 11.3.7, “Wi-Fi Management,” on page 82).

The Wi-Fi Security settings let you specify the minimum encryption that an access point must provide in order for the Security Client to allow a connection to the access point. Access points that do not meet the minimum security requirement are not displayed. If a user tries to manually define a connection to the access point, the connection is blocked.

For example, if you select WPA, any access points that provide less secure encryption (WEP 128, WEP 64, or no encryption) are blocked.

To configure the Wi-Fi Security settings:

1 In the Locations tree of the Management Console, click the + sign next to the location to expand the location settings, then select *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

Save complete

2 Select the *Minimum Security* level.

3 If you want to display a message to users when a connection fails because of insufficient security, select *Message if Minimum not met*, then fill in the message fields.

4 Click *Save Policy* to save your changes.

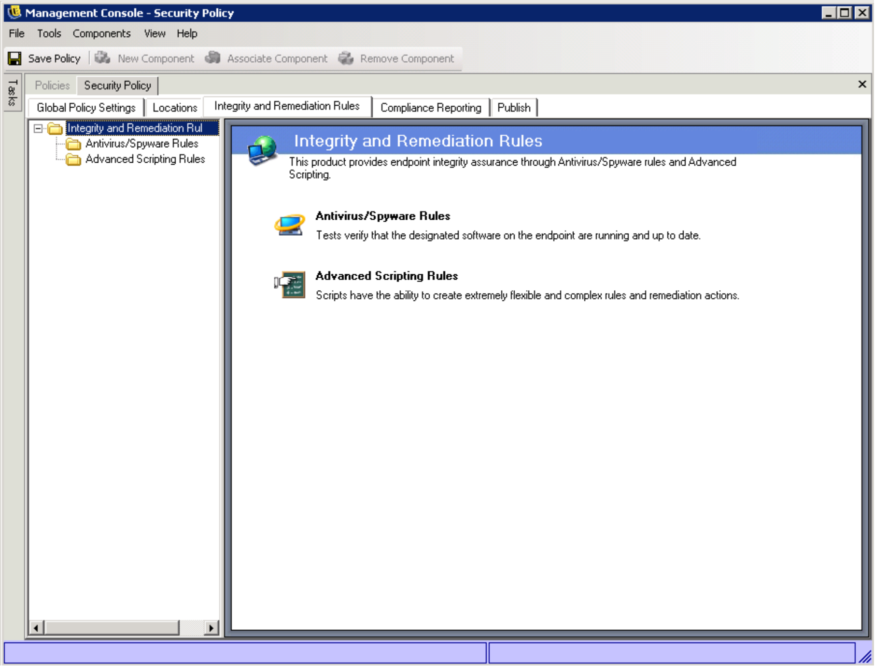
Configuring a Policy's Integrity and Remediation Rules

12

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.

To access the Integrity and Remediation Rules settings:

1. In the Management Console, double-click the policy in the Policies list.
2. Select the *Integrity and Remediation Rules* tab.



Integrity and Remediation Rules

This product provides endpoint integrity assurance through Antivirus/Spyware rules and Advanced Scripting.

Antivirus/Spyware Rules

Tests verify that the designated software on the endpoint are running and up to date.

Advanced Scripting Rules

Scripts have the ability to create extremely flexible and complex rules and remediation actions.

3. Configure the settings by referring to the following sections:
   - "Antivirus/Spyware Rules" on page 87
   - "Advanced Scripting Rules" on page 92

12.1 Antivirus/Spyware Rules

Antivirus/spyware rules verify that designated antivirus or spyware software on the endpoint device is installed, running. and up to date. Each rule includes one or more tests and each test can include two checks: File Exists (with date comparison) and Process is Running. If either check fails, you can determine the follow-up action:

- 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 a follow-up test determines that endpoints are compliant, security settings automatically return to their original state.

Several predefined rules are provided for common antivirus/spyware software. The rules include integrity tests and checks that you can edit as necessary. We recommend that you add a predefined rule in order to better see how rules work and are configured.

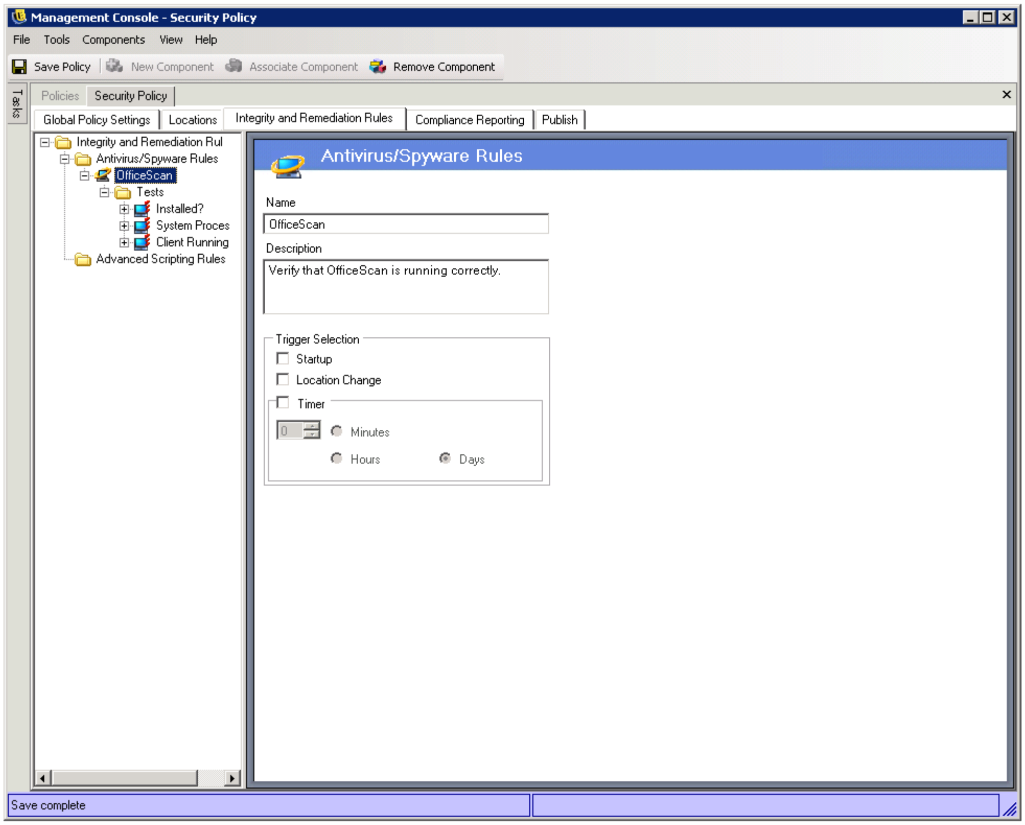
To add a rule:

1. In the Integrity and Remediation Rules tree of the Management Console, select the *Antivirus/Spyware Rules* folder.
2. If you want to define a new rule, click *New Component* on the Policy toolbar.

   or

   If you want to add an existing or predefined rule, click *Associate Component* on the Policy toolbar.

   The rule is added under the Antivirus/Spyware Rules folder in the tree. If you add a new rule, the name is displayed as *New Antivirus/Spyware Rules*. If you add an existing rule, the rule’s name is displayed.



Name: OfficeScan

Description: Verify that OfficeScan is running correctly.

Trigger Selection

□ Startup

□ Location Change

□ Timer

0 ○ Minutes

○ Hours ● Days

Save complete

3 Name the rule and provide a description.

4 Select the trigger for the rule:

- **Startup:** Run the tests at system startup.
- **Location Change:** Run the tests whenever the 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* to save your changes.

6 Continue with the next section, Integrity Tests, to define the rule's tests.

12.1.1 Integrity Tests

Each integrity test can run two checks, *File Exists* and *Process Running*. Each test has its own success and fail results. A single test can run checks for one or more software pieces within the same rule.

If you add multiple tests, the tests are run in the order listed, from top to bottom. The first test must finish successfully before the next test runs.

To add an integrity test:

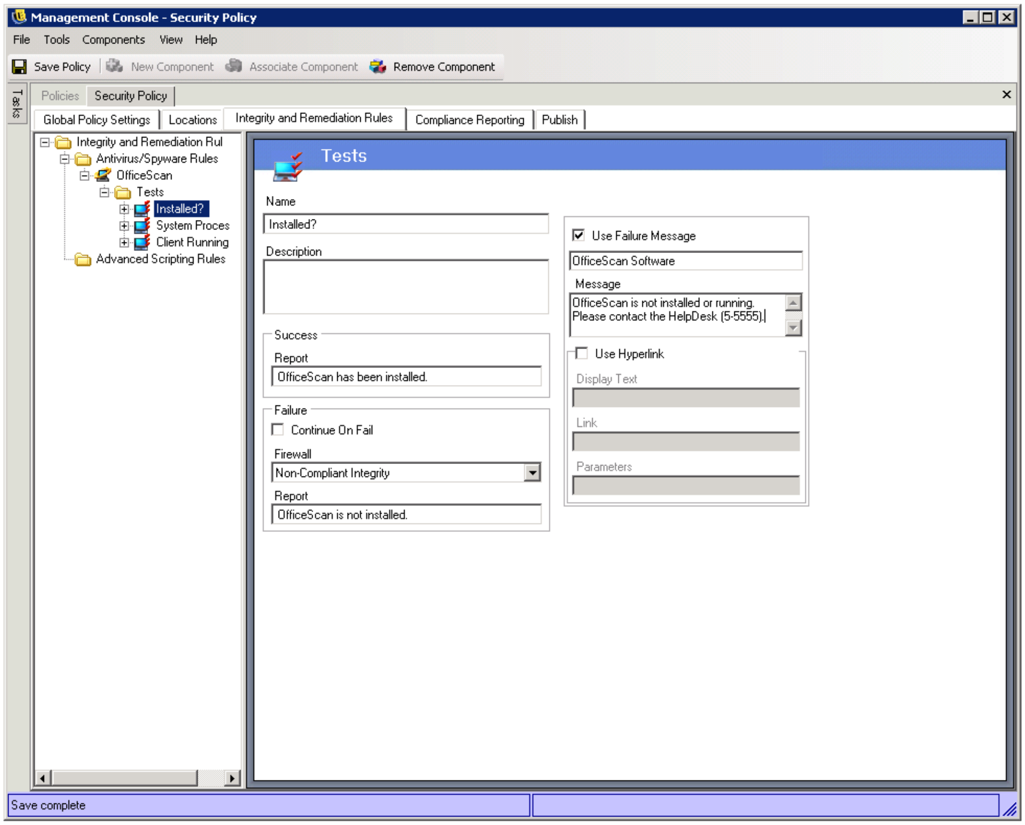
1 In the Integrity and Remediation Rules tree of the Management Console, click the + sign next to the rule to expand the rule settings, then select the *Tests* folder.

2 If you want to define a new test, click *New Component* on the Policy toolbar.

or

If you want to add an existing or predefined test, click *Associate Component* on the Policy toolbar.

The test is added under the Tests folder in the tree. If you add a new test, the name is displayed as *New Tests*. If you add an existing test, the test's name is displayed.



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

Display Text:

Link:

Parameters:

Save complete

3 Name the test and provide a description.

4 Provide the success report text for the test.

5 Define the following for a test failure:

- **Continue on Fail:** Select this option if you want the user to be able to continue to connect to network if the test fails. Deselect the option if the test should repeat.
- **Firewall:** This setting is applied if the test fails. All Closed, Non-compliant Integrity, or custom Quarantine firewall settings prevent 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.

6 Provide the title and message text for a failure message. This message displays only when one or more of the checks fail. Click the check box, then specify the information in the provided boxes.

7 Add a hyperlink 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.

8 Click *Save Policy* to save your changes.

9 Repeat Step 1 through Step 8 to create additional tests.

10 Continue with the next section, Integrity Checks, to define the test's checks.

12.1.2 Integrity Checks

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

To add an integrity check:

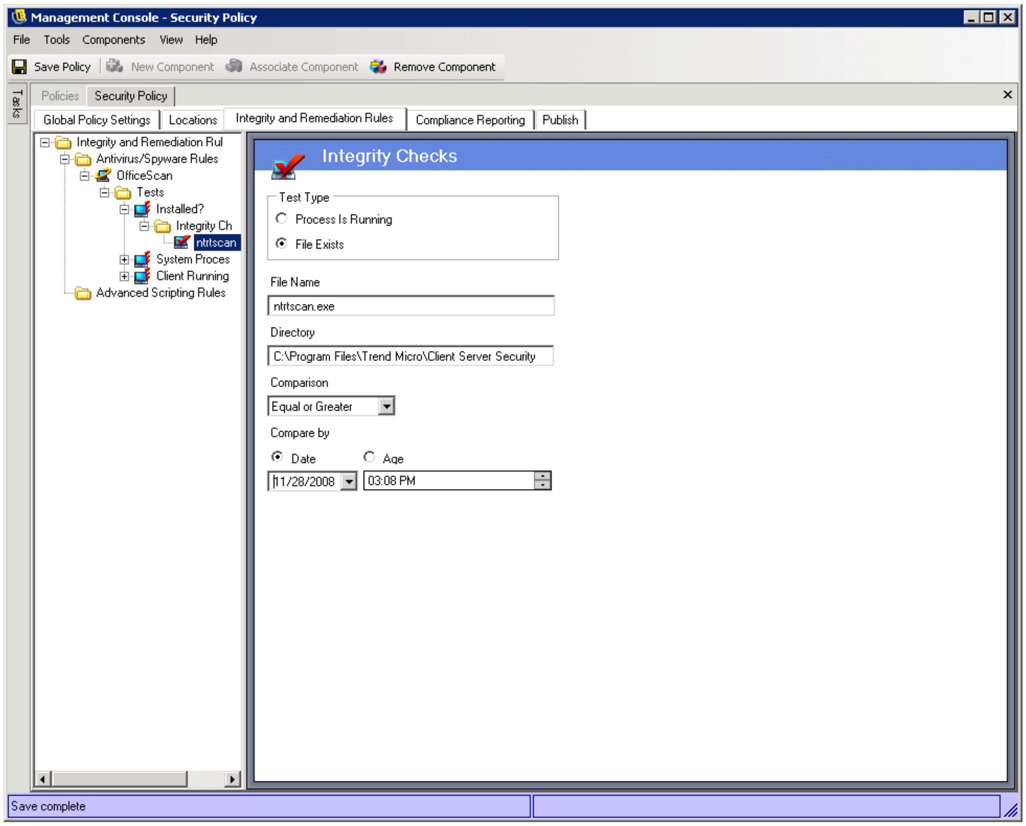
1 In the Integrity and Remediation Rules tree of the Management Console, click the + sign next to the test to expand the test settings, then select the *Tests* folder.

2 If you want to define a new check, click *New Component* on the Policy toolbar.

or

If you want to add an existing or predefined check, click *Associate Component* on the Policy toolbar.

The check is added under the Integrity Checks folder in the tree. If you add a new check, the name is displayed as *New Integrity Checks*. If you add an existing check, the check's name is displayed.



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

3 Configure the following settings:

- **Test Type:** Select the type of check:
  - **Process is Running:** Determines if the software is running at the time of the triggering event (such as the AV client). The only information required for this check is the executable name.
  - **File Exists:** Determines if the software is current and up-to-date at the time of the triggering event.

- **File Exists:** Determines if the software is current and up-to-date at the time of the triggering event.
- **File Name:** Specify the filename that you want to check. The filename is also used as the name of the integrity check.
- **Directory:** This setting applies only to the *File Exists* type. Specify the directory where the file resides.
- **Comparison:** This setting applies only to the *File Exists* type. If you want to perform a date comparison on the file, select the comparison, then fill in the *Compare by* fields.

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

4 Click *Save Policy* to save your changes.

12.2 Advanced Scripting Rules

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

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).

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

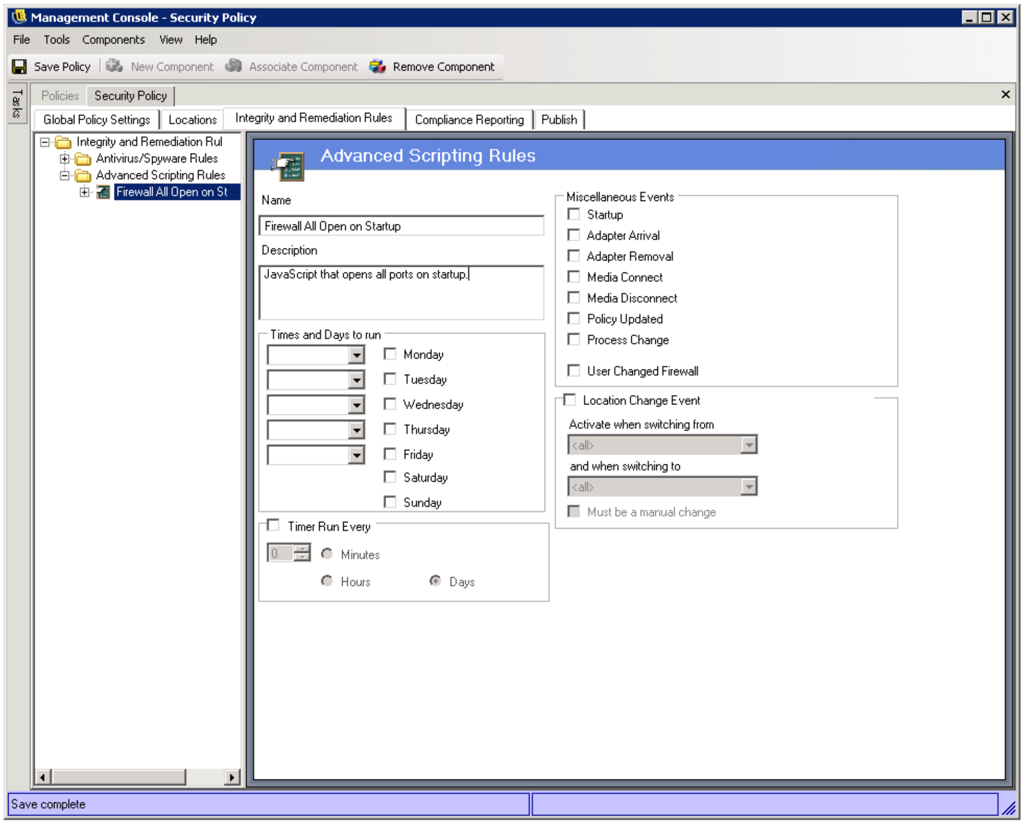
To add an advanced script:

1. In the Integrity and Remediation Rules tree of the Management Console, select the *Advanced Scripting Rules* folder.
2. If you want to define a new scripting rule, click *New Component* on the Policy toolbar.

   or

   If you want to add an existing or predefined scripting rule, click *Associate Component* on the Policy toolbar.

   The scripting rule is added under the Advanced Scripting Rules folder in the tree. If you add a new scripting rule, the name is displayed as *New Advanced Scripting Rules*. If you add an existing scripting rule, the scripting rule's name is displayed.



Advanced Scripting Rules

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

Save complete

3 Name the rule and provide a description.

4 Specify the triggering events:

- **Times and Days to Run:** Specify as many as five different times for the script to run. The script runs weekly on the selected days.
- **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.
  - **Activate when switching from:** The script runs whenever the user changes from this specified location to another location.
  - **Activate when switching to:** The script runs whenever the user changes to this specified location from any other location. If *Activate when switching from* was given a location (such as Office), the script runs only when the location switches from Office to this specified location.
  - **Must be a manual change:** The script runs only when the user manually switches from or to a location.

5 Create any script variables. For more information see "Script Variables" on page 94.

6 Write the script text. For more information, see "Script Text" on page 95.

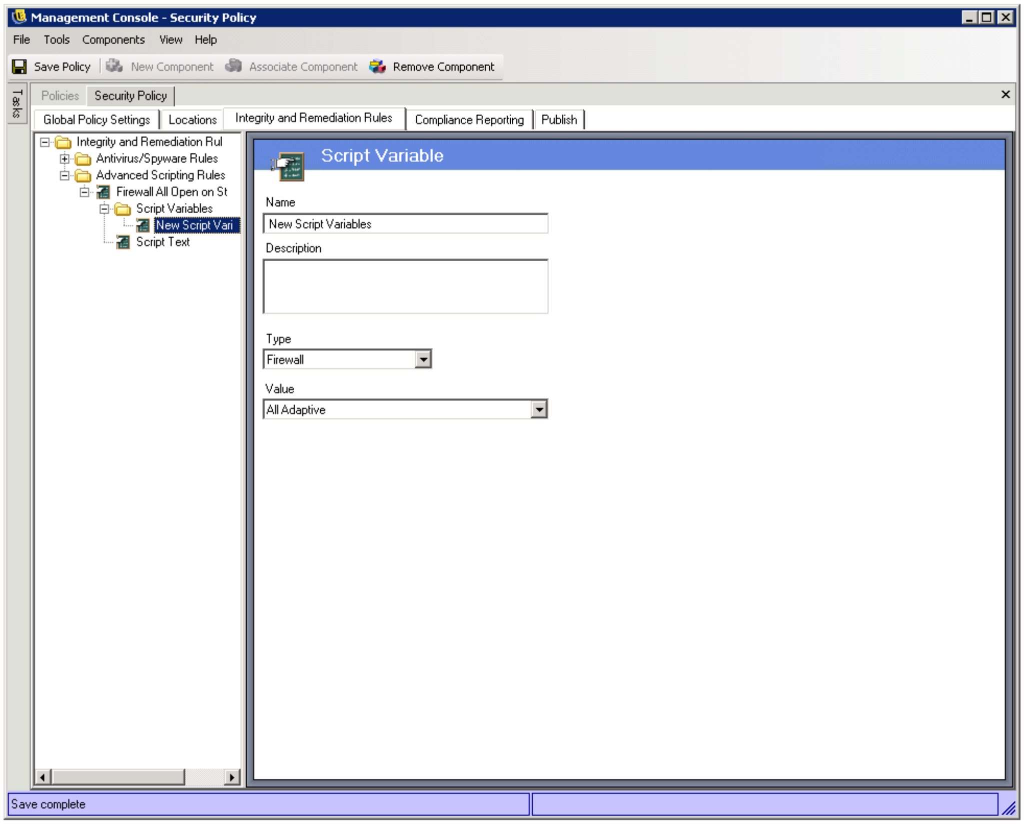
7 Click *Save Policy*.

12.2.1 Script Variables

This is an optional setting you can use to define a variable (var) for the script. The variable can include a firewall setting, a location, a number value, or a string value.

To create a new script variable:

1. In the Integrity and Remediation Rules tree of the Management Console, click the + sign next to the scripting rule to expand the rule settings, then select the *Script Variables* folder.
2. Click *New Component* to create a new script variable.



Name: New Script Variables

Description:

Type: Firewall

Value: All Adaptive

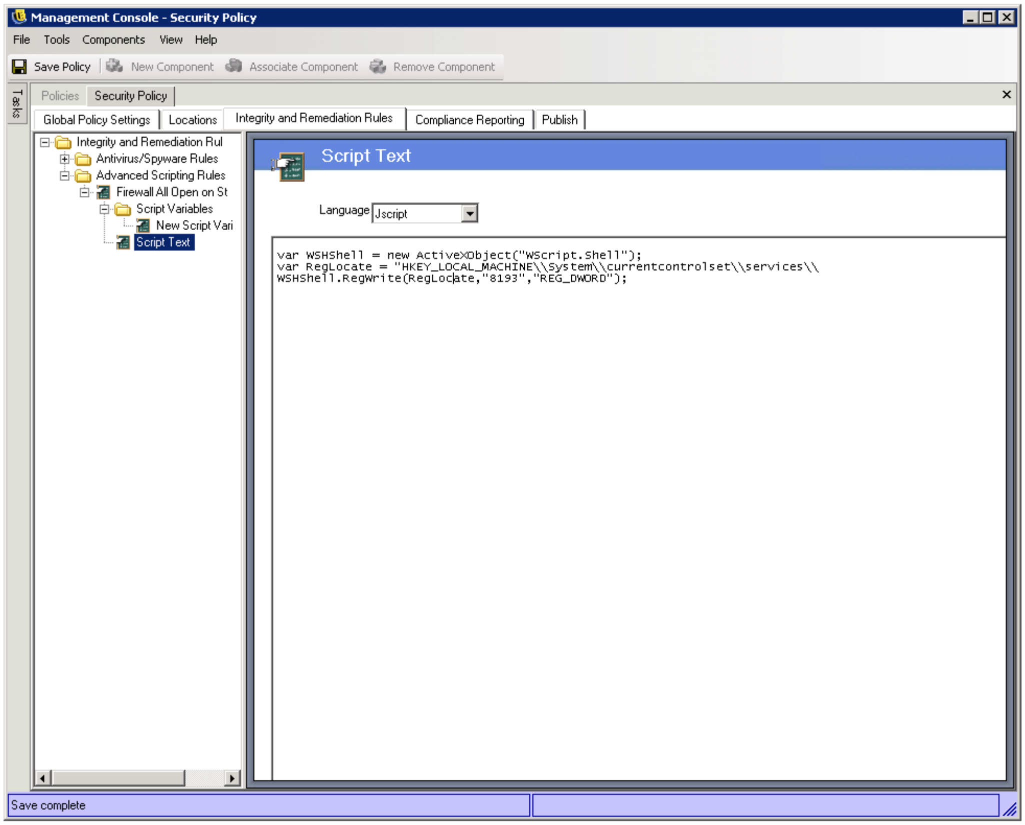
3. Name the variable and provide a description.
4. Select the type of variable:
   - **Firewall:** Defines a firewall setting that can be applied as an action.
   - **Location:** Defines a location that can be applied as an action.
   - **Number:** Defines a number value.
   - **String:** Defines a string value.
5. Specify the value of the variable.
6. Click *Save Policy* to save your changes.
7. Repeat Step 1 through Step 6 to create a new variable.

12.2.2 Script Text

It is strongly recommended that you test a script before distributing the policy.

To add the script text:

1. In the Integrity and Remediation Rules tree of the Management Console, click the + sign next to the scripting rule to expand the rule settings, then select *Script Text*.



Language Jscript

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

2. Select the script language (*Jscript* or *VBscript*).
3. Specify the script in the provided field.

   For information about creating scripts, including sample scripts you can reference, see Appendix D, “Advanced Scripting Rules,” on page 177.

Configuring a Policy’s Compliance Reporting

13

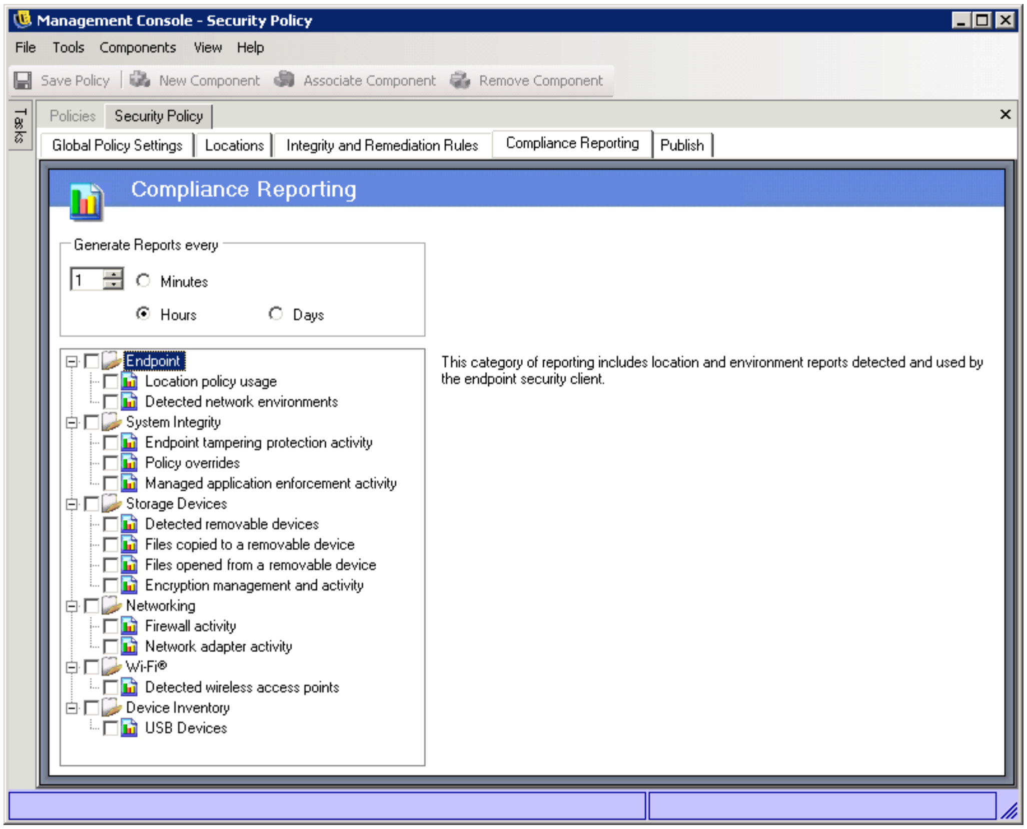
Because of the level and access of the Security Client's drivers, virtually every transaction the endpoint performs can be reported. In addition, the Security Client can create system inventory reports that you can use for troubleshooting problems and creating security policies.

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

To determine which reports are generated and how often they are generated:

1 In the Management Console, open the policy by double-clicking the policy in the *Policies* list.

2 Click the *Compliance Reporting* tab.



Generate Reports every

1 ○ Minutes

● Hours ○ Days

- □ Endpoint
  - □ Location policy usage
  - □ Detected network environments
- □ System Integrity
  - □ 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
- □ Networking
  - □ Firewall activity
  - □ Network adapter activity
- □ Wi-Fi®
  - □ Detected wireless access points
- □ Device Inventory
  - □ USB Devices

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

3 In the *Generate Reports every* field, specify how often you want the Security Client to generate reports and upload them to the Policy Distribution Service.

4 Select the reports you want generated. The reports are described below:

Endpoint

- **Location policy usage:** The Security Client reports all location policies enforced and the duration of that enforcement.

- **Detected network environments:** The Security Client reports all detected network environment settings.

System Integrity

- **Endpoint tampering protection activity:** The Security Client reports any attempts to tamper with it.
- **Policy overrides:** The Security Client reports all attempts to initiate the administrative override on it.
- **Managed application enforcement activity:** The Security Client reports all enforcement activities for managed applications.

Storage Devices

- **Detected removable devices:** The Security Client reports all removable storage devices detected by the security client.
- **Files copied to a removable device:** The Security Client reports files that are copied to a removable storage device.
- **Files opened from a removable device:** The Security Client reports files that are opened from a removable storage device.
- **Encryption management and activity:** The Security Client reports its encryption/decryption activity.

Networking

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

  IMPORTANT: This data can overwhelm a database very quickly. A test of one Security Client reported 1,115 data uploads of blocked packets over a 20-hour period. You should run a monitoring and tuning period with a test Security Client in the deployment environment prior to wide-scale use of this report.

- **Network adapter activity:** The Security Client reports all traffic activity for a managed network device.

Wi-Fi

- **Detected wireless access points:** The Security Client reports all detected access points.

Device Inventory

- **USB Devices** The Security Client reports all USB devices.

Distributing a Policy

14

After you create and configure a security policy, you need to distribute it to users or computers.

The method you use to distribute policies depends on whether your ZENworks® Endpoint Security Management system uses the Management Service and the Policy and Distribution Service. If your system includes the two services, you *publish* policies and the services deliver the policies. If your system does not include the services, you *export* policies and then manually deliver them.

The following sections provide information for both methods:

- Section 14.1, "Publishing a Policy," on page 99
- Section 14.2, "Republishing an Updated Policy," on page 100
- Section 14.3, "Exporting a Policy," on page 102

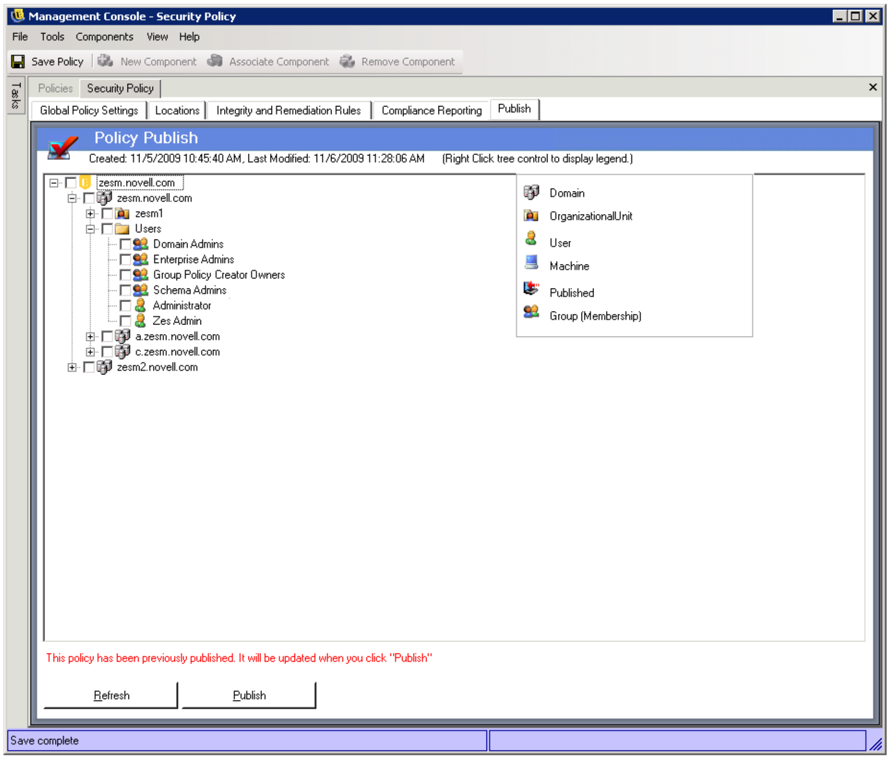
14.1 Publishing a Policy

If your ZENworks Endpoint Security Management system includes the Management Service and Policy Distribution Service, complete the following steps to publish a policy to your endpoint devices.

If your system does not include the services, you must export policies and then manually deliver them. Skip to Section 14.3, "Exporting a Policy," on page 102.

To publish a policy:

1. In the Management Console, open the policy.
2. Click the *Publish* tab.



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

The Policy Publish page displays the directory service trees to which the system has connections.

3 Select the users, computers, or groups to which you want to publish the policy.

Keep in mind the following:

- If you select an entire domain or organizational unit, the policy is published to all users and computers within the domain or unit.
- If a directory object is displayed in red, your Management Console login account does not provide rights to publish to that object.
- If the directory tree does not display the users, computers, or groups to which you want to publish the policy, you might need to synchronize the Management database with the directory service. Users and computers are not added to the Management database until 1) they are synchronized from the directory service or 2) they log in via the Security Client for the first time. For information about synchronizing the database, see Chapter 3, "Configuring Data Synchronization Schedules," on page 25.
- If you need to clear your selected objects, click *Refresh*.

4 Click *Publish*.

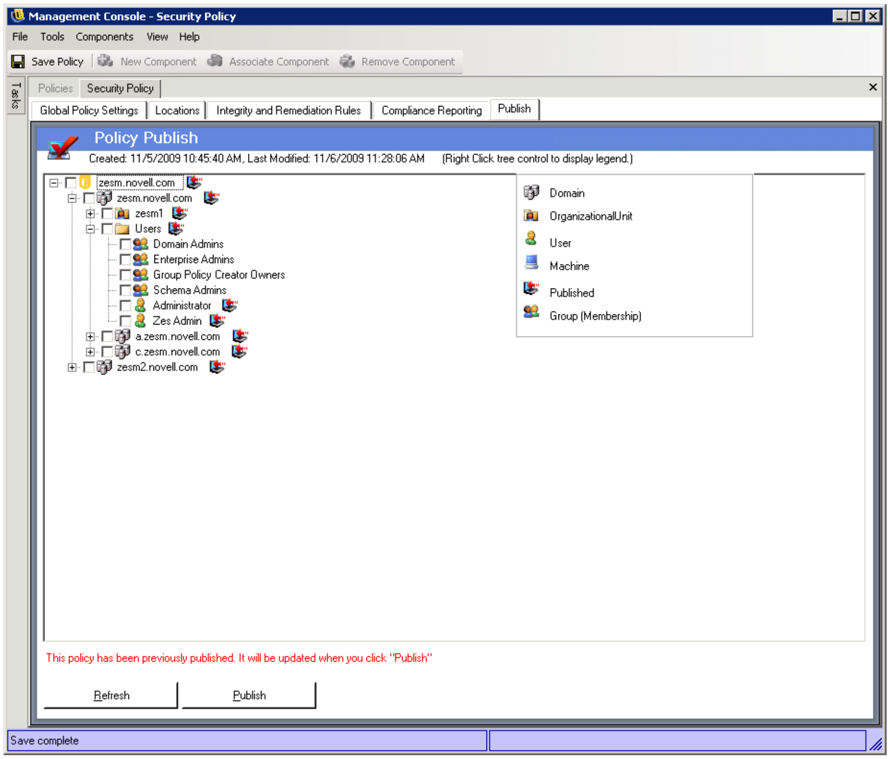
14.2 Republishing an Updated Policy

After a policy has been published to users or computers, you must republish the policy if you make any changes to it.

For example, if you change the WEP key for an access point, you need to save the policy and then publish it again. Any user or computer to which the policy was previously published receives the updated policy the next time the Security Client checks in.

1 In the Management Console, open the policy.

2 Click the *Publish* tab.



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"

The Policy Publish page displays the directory service trees to which the system has connections. The 🖥 icon indicates the objects to which the policy was previously published. You do not need to reselect these objects. The policy will automatically be republished to them.

3 If there are additional users, computers, or groups to which you want to publish the policy, select those objects.

Keep in mind the following:

- If you select an entire domain or organizational unit, the policy is published to all users and computers within the domain or unit.
- If a directory object is displayed in red, your Management Console login account does not provide rights to publish to that object.
- If the directory tree does not display the users, computers, or groups to which you want to publish the policy, you might need to synchronize the Management database with the directory service. Users and computers are not added to the Management database until 1) they are synchronized from the directory service or 2) they log in via the Security Client for the first time. For information about synchronizing the database, see Chapter 3, "Configuring Data Synchronization Schedules," on page 25.
- If you need to clear your selected objects, click *Refresh*.

4 Click *Publish*.

14.3 Exporting a Policy

If your ZENworks Endpoint Security Management system does not include the Management Service and the Policy Distribution Service, you must export a policy from your stand-alone Management Console and then manually deliver it to endpoint devices.

To export a policy:

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. In the Management Console, open the policy.
3. Click *File* > *Export Policy*.
4. Specify the name and location for the file, then click *Export*.

   For the location, specify the same folder containing the `setup.sen` file (see Step 1). For the name, specify `policy.sen`.. All policies distributed must be named `policy.sen` in order for the Security Client to accept them.
5. Distribute the `policy.sen` and `setup.sen` files to endpoint devices.

   These files must be copied to the `\Program Files\Novell\ZENworks Security Client` directory

   The `setup.sen` file needs to be copied to endpoint devices only once with the first policy. Afterwards, only new (or updated) policies need to be distributed.

NOTE: There are multiple methods you can use to distribute the policy to a Security Client located on the same machine as the standalone Management Console.

If the Security Client was installed on the machine after the standalone Management Console, the file must be exported and transferred manually as described above.

If the Security Client was installed on the machine before the standalone Management Console, you can follow the steps above to export the policy, or you can publish the policy. To publish the policy, click *File* > *Publish*.

Importing and Exporting Policies 15

If you need to send policies to another ZENworks® Endpoint Security Management system, or if you want to back up your policies, you can export them. You can also import policies you receive or policies you export for backup purposes.

The following sections contain instructions:

- Section 15.1, "Importing Policies," on page 103
- Section 15.2, "Exporting a Policy," on page 103

IMPORTANT: For information about exporting polices to distribute to endpoint devices, see Chapter 14, "Distributing a Policy," on page 99.

15.1 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 if necessary) before opening the Import a Policy dialog box.

2 In the *File Name & Location* field, click the browse button to select the policy file to import.

3 Click *Import*.

After the policy is imported, it can be further edited or immediately published.

15.2 Exporting a Policy

Policies can be exported from the Management Console and distributed via e-mail or through a network share. This lets you share policies between two or more ZENworks Endpoint Security Management systems.

To export a policy:

1 In the Management Console, make sure the policy you want to export is open.

2 Click *File* > *Export*.

3 In the *File Name & Location* field, specify a destination and give the policy a name with an extension of `.sen` (for example, `C:\Desktop\salespolicy.sen`) If necessary, click the browse button to browse to a location.

4 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.

Security Client

III

The ZENworks® Endpoint Security Management Client, referred to as the *Security Client*, enforces security policies on endpoint devices.

The following sections provide information to help you manage the Security Client. For information about using the Security Client, see the *ZENworks Endpoint Security Client for Windows 2000/XP User Guide* and the *ZENworks Endpoint Security Client for Windows Vista/7 User Guide*.

About the Security Client

16

Novell® ZENworks® Endpoint Security Management uses the Security Client, installed on endpoint devices, to enforce security on the devices. There are two versions of the client: the Windows 2000/XP Security Client and the Windows Vista/7 Security Client. For operating system support and client requirements, see "System Requirements" in the *ZENworks Endpoint Security Management 4.1 Installation Guide*.

16.1 What the Security Client Does

The Security Client receives the security policies that you create and enforces the policies on the endpoint device. This includes the following:

- Enforcing the policy's global settings. These are settings intended to be applied regardless of the device's location.
- Determining the device's location and enforcing the security settings defined for that location.
- Securing wireless connectivity through the control of wireless network adapters and wireless access points.
- Controlling the availability of communication hardware, such as Bluetooth and IrDA.
- Controlling the use of USB devices.
- Providing data encryption for both fixed drives and removable storage devices.
- Validating the status and operation of anti-virus/spyware software.
- Collecting security-centric statistics and event traps, and passing that information to the ZENworks Endpoint Security Management system for analysis through the Management Console.

All Security Client functionality is determined by the security policy. For information about creating security policies, see Part II, "Security Policies," on page 37.

16.2 Security Client Differences Based on Windows Version

The Security Client runs on Windows 2000, Windows XP, Windows Vista, and Windows 7 (see "System Requirements" in the *ZENworks Endpoint Security Management 4.1 Installation Guide* for detailed version requirements). However, because of differences in these versions of the Windows operating system, not all features are supported on all versions. The following table lists the feature support for each Windows version.

	Windows 2000	Windows XP	Windows Vista/7
LOCATION AWARENESS			
Enforce security policy settings by location	✓	✓	✓
Allow manual location change	✓	✓	✓
Allow saving of network environment to associate network environment with current location	✓	✓	
Allow manual change of firewall settings (if multiple firewall settings exist)	✓	✓	
CLIENT SELF DEFENSE			
Require an uninstall Password	✓	✓	✓
Block the termination of client processes via Task Manager	✓	✓	✓
Block the stopping/pausing of the client via Service Manager	✓	✓	✓
Protect client files and registry entries	✓	✓	
Automatically rebind of the NDIS filter driver	✓	✓	
STORAGE DEVICE CONTROL			
Control optical writer (CD/DVD) access (R, R/W, no access)	✓	✓	✓
Control floppy drive access (R, R/W, no access)	✓	✓	✓
Control AutoPlay/AutoRun access	✓	✓	✓
Control removable storage device access (R, R/W, no access)	✓	✓	✓
Create removable storage device approval lists	✓	✓	✓
WIRELESS CONTROL			
Enforce wireless card (adapter) approval lists	✓	✓	✓
Disable wireless transmissions by disabling all wireless cards (adapters)	✓	✓	✓
Block wireless connections but keep Wi-Fi radio active		✓	
Disable wireless transmissions when wired	✓	✓	✓

	Windows 2000	Windows XP	Windows Vista/7
Disable ad hoc wireless connections		✓	✓
Disable adapter bridging		✓	✓
Automate WEP pre-shared key distribution for access points		✓	
Filter and prohibit access points		✓	
Enforce connection preference based on access point security levels or signal strengths		✓	
DATA ENCRYPTION			
Provide a “safe harbor” encrypted folder on fixed disks		✓	✓
Encrypt the “My Documents” folder		✓	
Enable user-defined encrypted folders on fixed disks		✓	✓
Encrypt removable storage devices		✓	✓
Share password-protected encrypted files by using administrator-distributed decryption utility		✓	✓
FIREWALL PROTECTION			
Set default behavior to open, closed, or stateful	✓	✓	✓
Enforce TCP/UDP ports and protocols access rules	✓	✓	✓
Enforce access control lists (ACLs) for IP and MAC addresses.	✓	✓	✓
Allow multiple firewall settings within a location	✓	✓	
Allow manual change of firewall setting within a location	✓	✓	
VPN ENFORCEMENT			
Require and automate launch of a VPN client based on location	✓	✓	✓
Enforce VPN authentication timeouts	✓	✓	
Control wired, wireless, and dial-up adapter access	✓	✓	
APPLICATION CONTROL			
Block application execution	✓	✓	

	Windows 2000	Windows XP	Windows Vista/7
Block application access to Internet	✓	✓	
COMMUNICATION HARDWARE CONTROL			
Control access to 1394 (FireWire), irDA (infrared), Bluetooth, and Serial/ Parallel communication	✓	✓	✓
Control wired communication, including enforcement of wired adapter approval list	✓	✓	✓
Control dialup (modem) communication, including enforcement of dialup adapter approval list	✓	✓	
Enforce wireless adapter approval list	✓	✓	✓
USB CONNECTIVITY			
Control access based on USB device groups (mass storage, printers, etc.)		✓	
Control access to individual devices		✓	
CLIENT UPDATE			
Enforce Security Client update policy	✓	✓	
INTEGRITY AND REMEDIATION			
Verify that required antivirus and spyware software is running and up to date.	✓	✓	
Enforce remediation proceduresif software fails verification	✓	✓	
Support advanced scripting for softwre integrity checks and remediation	✓	✓	
COMPLIANCE REPORTING AND ALERTS			
Supply data to Management Console for reporting on security policy compliance	✓	✓	
Supply data to Management Console for monitoring of security threats	✓	✓	

16.3 Security Client Self Defense

The Security Client includes the ability to protect itself 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 a password.

- Windows Task Manager requests to terminate `STEngine.exe` and `STUser.exe` processes are disallowed.
- 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.

Security Client Self Defense is enabled and configured as part of the security policy. For information, see Section 10.2, "Policy Settings," on page 42.

16.4 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 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.

Because only one policy can be enforced at a time, Microsoft Fast User Switching (FUS) is not supported. The Security Client turns off FUS at installation.

For an unmanaged client (one not connected to a Policy Distribution Service), 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.

16.5 Machine-Based Policies

The option for using machine-based rather than user-based policies is set at Security Client installation (see the *ZENworks Endpoint Security Management 4.1 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 a 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.

17 Installing the Security Client

Detailed installation instructions are provided in "Installing the Security Client" in the *ZENworks Endpoint Security Management 4.1 Installation Guide*.

Updating the Security Client 18

The following sections explain different methods you can use to update the Security Client from one release to another:

- Section 18.1, "Using a Policy's ZSC Update Setting," on page 115
- Section 18.2, "Using the Installation Program's Upgrade Switch," on page 115
- Section 18.3, "Using an MSI Uninstall and Reinstall," on page 115

18.1 Using a Policy's ZSC Update Setting

A security policy includes a ZSC Update setting that you can use to update the client.

1. Configure the policy's ZSC Update setting. For instructions, see Section 10.8, "ZSC Update," on page 56.
2. Republish the policy to endpoint devices. For instructions, see Section 14.2, "Republishing an Updated Policy," on page 100.

18.2 Using the Installation Program's Upgrade Switch

The Security Client installation program (`setup.exe`) includes an upgrade switch. The command syntax is:

```
setup.exe /V"STUPGRADE=1"
```

There are different ways you can run the command syntax:

- Create a desktop shortcut to the `setup.exe` program on the installation media, then modify the shortcut target to include the switch.
- Run `setup.exe /V"STUPGRADE=1"` at a command line prompt.

18.3 Using an MSI Uninstall and Reinstall

You cannot use MSI to perform an in-place upgrade of the Security Client. However, you can use it to uninstall the current Security Client and install the new Security Client.

1. Uninstall the Security Client. See Chapter 19, "Uninstalling the Security Client," on page 117.
2. Install the Security Client. See "Installing the Security Client" in the *ZENworks Endpoint Security Management 4.1 Installation Guide*.

Uninstalling the Security Client

19

The following sections provide instructions for uninstalling the Security Client:

- Section 19.1, "Preparing a Machine for Client Uninstallation," on page 117
- Section 19.2, "Performing an Attended Uninstall," on page 117
- Section 19.3, "Performing an Unattended (Silent) Uninstall," on page 118

19.1 Preparing a Machine for Client Uninstallation

Before uninstalling the Security Client on a machine, you should do the following:

- On the machine, move any files from encrypted safe harbor locations to unencrypted locations. This decrypts the files and ensures that they will be available after the client is uninstalled. In addition, you should export the encryption keys in case any orphaned encrypted files remain; the encryption keys can then be used with the decryption utility to decrypt the files. For help exporting the encryption keys, see Section 7.1, "Exporting Encryption Keys," on page 33. For help using the decryption utility, see Chapter 24, "ZENworks File Decryption Utility," on page 163.
- Distribute a simple policy to the machine. Have the policy disable encryption and enable communication hardware and storage devices.
- 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).

19.2 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"
  ```
- Windows 2000 and Windows XP: Run Windows Installer, using the following command syntax:

  ```
  msiexec.exe /x {C1773AE3-3A47-48EB-9338-7FF2CDC73E67} STUNINSTALL=1
  ```
- Windows Vista and Windows 7: Run Windows Installer, using the following command syntax:

  ```
  msiexec.exe /x {6208B443-6136-484A-AF4A-74BEA8A3840E} STUNINSTALL=1
  ```

The following table lists additional command line variables that you can use during an uninstall:

Command Line Variable	Description
STUIP=*password*	Specifies the password required to uninstall the Security Client. Example: `setup.exe /V"STUNINSTALL=1 STUIP=removeZESM"`
STPROMPT=1	Decrypts the encrypted files in any safe harbor locations. This switch is not recommended. If you use it, you need to ensure that no encrypted files are open (i.e., no open file handles) and that the uninstall program completes before the computer is shut down. If either of these conditions occur, the uninstall fails. The strongly recommended approach is to have users decrypt files before the uninstall by manually moving the encrypted files from safe harbor locations to other locations. Example: `setup.exe /V"STUNINSTALL=1 STPROMPT=1"`

19.3 Performing an Unattended (Silent) Uninstall

To perform a silent uninstall of 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"
  ```

- Windows 2000 and Windows XP: Run Windows Installer, using the following command syntax:

  ```
  msiexec.exe /x /qn {C1773AE3-3A47-48EB-9338-7FF2CDC73E67} STUNINSTALL=1
  ```

- Windows Vista and Windows 7: Run Windows Installer, using the following command syntax:

  ```
  msiexec.exe /x /qn {6208B443-6136-484A-AF4A-74BEA8A3840E} STUNINSTALL=1
  ```

The following table lists additional command line variables that you can use during an uninstall:

Command Line Variable	Description
STUIP=*password*	Specifies the password required to uninstall the Security Client. Examples: `setup.exe /s /x /V"/qn STUNINSTALL=1 STUIP=removeZESM"` `msiexec.exe /x /qn {C1773AE3-3A47-48EB-9338-7FF2CDC73E67} STUNINSTALL=1` STUIP=removeZESM

Command Line Variable	Description
STPROMPT=1	Decrypts the encrypted files in any safe harbor locations. This switch is not recommended. If you use it, you need to ensure that no encrypted files are open (i.e., no open file handles) and that the uninstall program completes before the computer is shut down. If either of these conditions occur, the uninstall fails. The strongly recommended approach is to have users decrypt files before the uninstall by manually moving the encrypted files from safe harbor locations to other locations. Examples: `setup.exe /s /x /V"/qn STUNINSTALL=1 STPROMPT=1"` `msiexec.exe /x /qn {C1773AE3-3A47-48EB-9338-7FF2CDC73E67} STUNINSTALL=1` STPROMPT=1

Using the Security Client Diagnostic Tools 20

The 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.

- Section 20.1, "Windows 2000/XP Security Client Diagnostics Tools," on page 121
- Section 20.2, "Windows Vista/7 Security Client Diagnostic Tools," on page 129

20.1 Windows 2000/XP Security Client Diagnostics Tools

The following sections explain the diagnostic tools available in the Windows 2000/XP version of the Security Client:

- Section 20.1.1, "Creating a Diagnostics Package," on page 121
- Section 20.1.2, "Administrator Views," on page 123
- Section 20.1.3, "Logging," on page 127
- Section 20.1.4, "Reporting," on page 128

20.1.1 Creating a Diagnostics Package

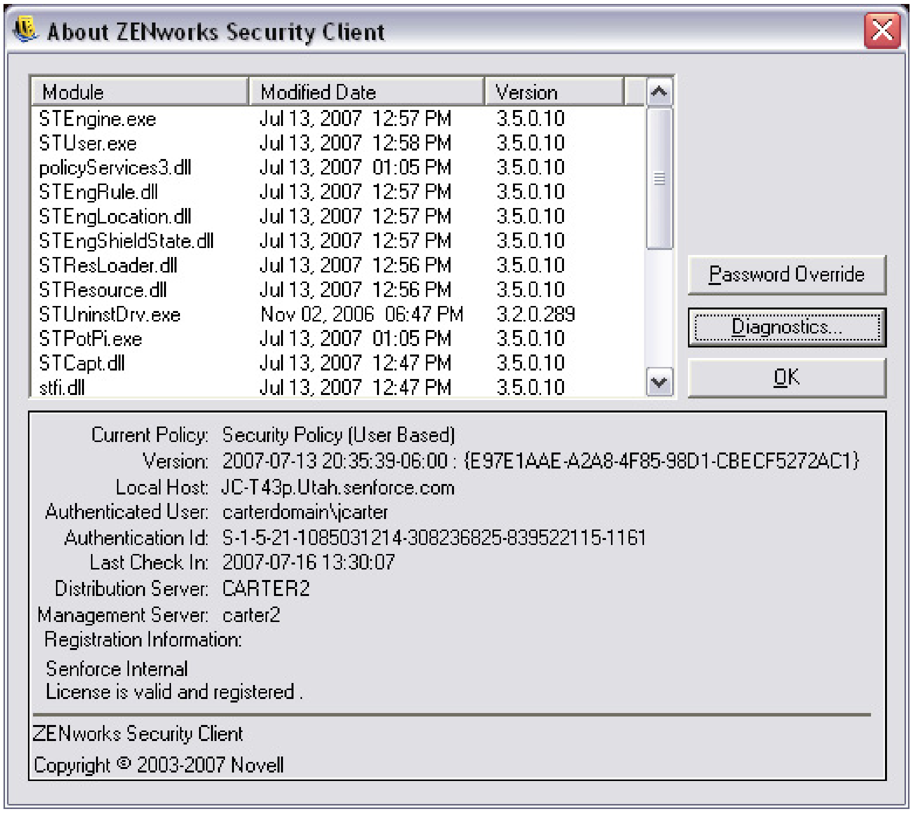
If problems occur because of the Security Client's presence on the endpoint device, administrators can provide detailed diagnostics information packages to Novell Support. This information is vital in resolution of any issues. The diagnostics package is defined by the following items:

- **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 "Logging" on page 127).
- **Policy:** Captures the current policy running on the Endpoint Security Client (see "View Policy" on page 123).
- **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 "Reporting" on page 128).
- **System Event Logs:** Captures the current System Event logs.

- **System Information:** Captures all system information.

To create a diagnostics package:

1 On the endpoint device, right-click the *Security Client* icon, then click *About*.

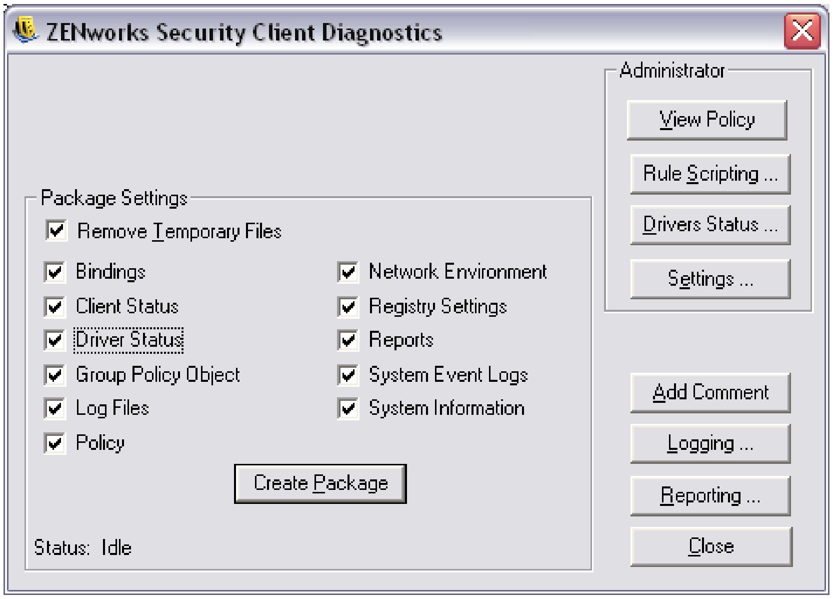


Module	Modified Date	Version
STEngine.exe	Jul 13, 2007 12:57 PM	3.5.0.10
STUser.exe	Jul 13, 2007 12:58 PM	3.5.0.10
policyServices3.dll	Jul 13, 2007 01:05 PM	3.5.0.10
STEngRule.dll	Jul 13, 2007 12:57 PM	3.5.0.10
STEngLocation.dll	Jul 13, 2007 12:57 PM	3.5.0.10
STEngShieldState.dll	Jul 13, 2007 12:57 PM	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*.



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

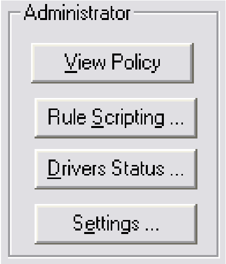
3. Select the items to be included in the package (all are selected by default).
4. Click *Create Package* to generate the package.

   The generated package (`ESSDiagnostics_YYYYMMDD_HHMMSS.zip.enc`) is available on the desktop. This encrypted zip file can now be sent to Novell 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.

20.1.2 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.

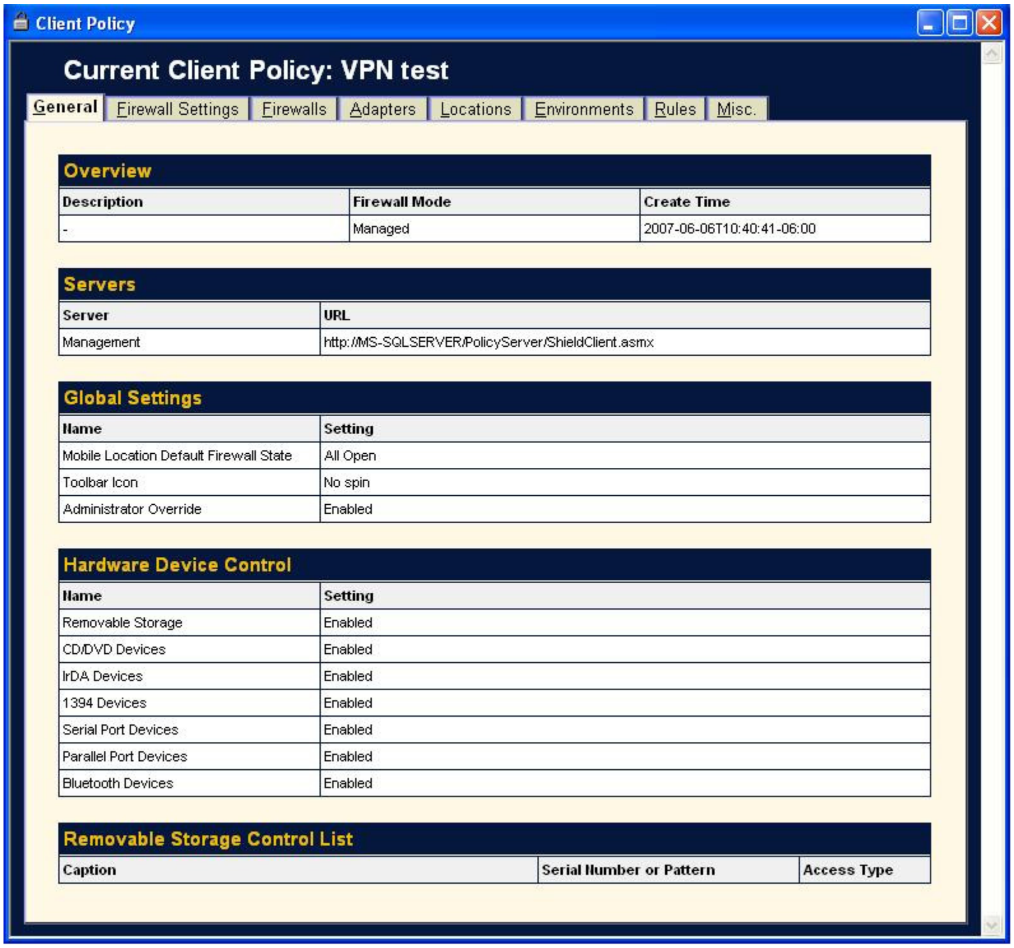


The following sections contain more information:

- "View Policy" on page 123
- "Rule Scripting" on page 124
- "Driver Status" on page 125
- "Settings" on page 126

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.



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

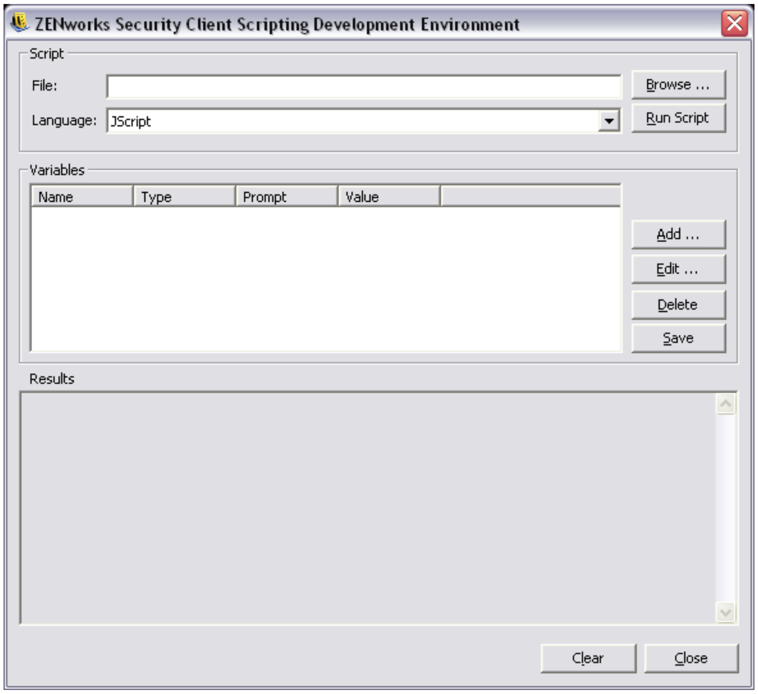
Caption	Serial Number or Pattern	Access Type

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.

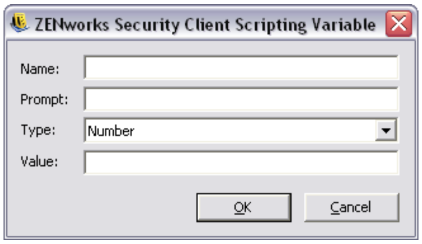
Rule Scripting

The *Rule Scripting* button allows the administrator to enter a specific script into the Security Client. The script runs only on this endpoint. 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.



Language: JScript

Variables are created by clicking *Add*, which displays a second window where the variable information can be entered.

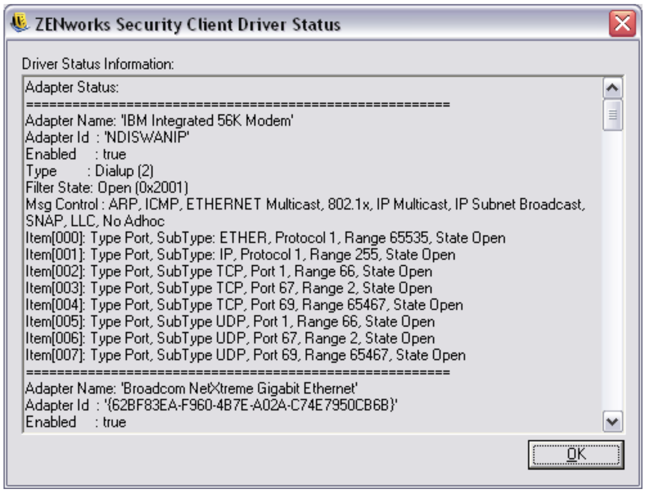


Type: Number

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.

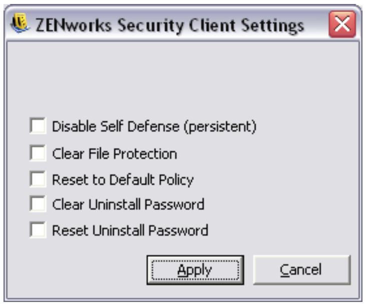


Driver Status Information:

```
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.



☐ 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 126
- "Clear File Protection" on page 126
- "Reset to Default Policy" on page 127
- "Clear Uninstall Password" on page 127
- "Reset Uninstall Password" on page 127

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

Clears the hashes from the protected files. The current policies and licensing information remains. After the hashes are cleared, the file can 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

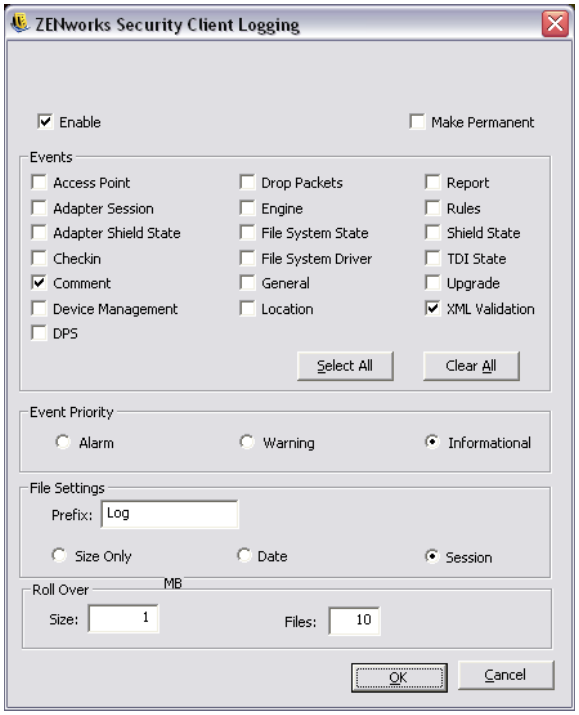
Clears the password that is required for uninstalling the Security Client. After the password is cleared, the Security Client can be uninstalled without a password prompt. Use this option when the uninstall password fails or is lost.

Reset Uninstall Password

Resets the password required to uninstall the Security Client. You are prompted to enter the new uninstall password.

20.1.3 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, you should set logging according to the directions of Novell Support and repeat the circumstances that led to the error.



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

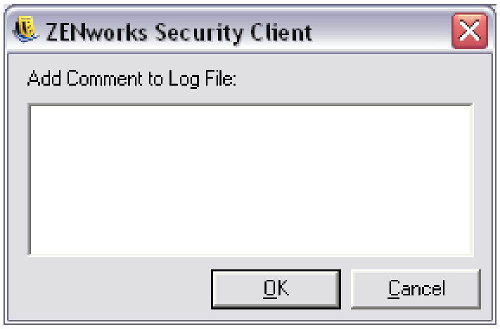
Size: 1 MB Files: 10

Additionally, the type of log created, file settings, and roll-over settings can be adjusted, based on your current needs.

To retain the new log settings after the device's reboot, select the *Make Permanent* box; otherwise the Security Client reverts to its default logs at the next reboot.

Add Comment

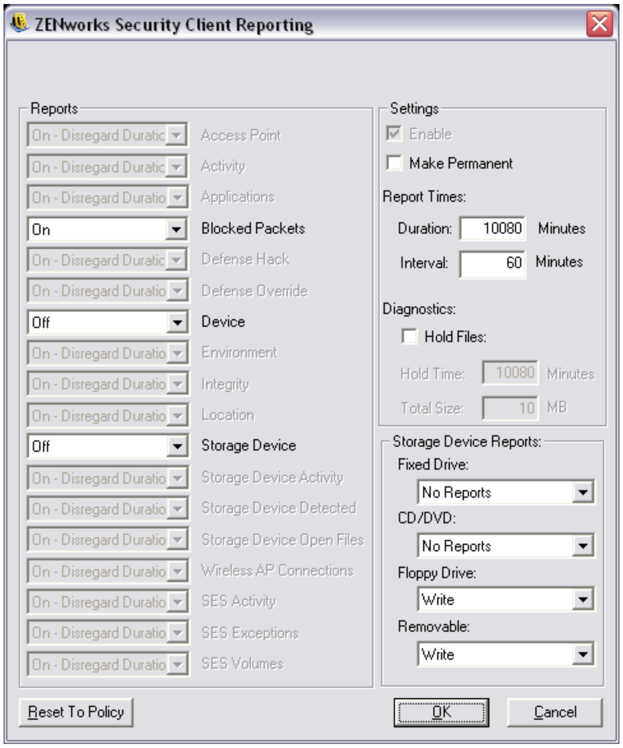
The option to add a comment to the logs is available on the diagnostics window. Click the *Add Comments* button to display the Add Comment window. Comments are included with the next batch of logs.



NOTE: If the *Comments* option in logging is deselected, the *Add Comments* button does not display.

20.1.4 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 13, "Configuring a Policy's Compliance Reporting," on page 97 for descriptions of the report types.



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

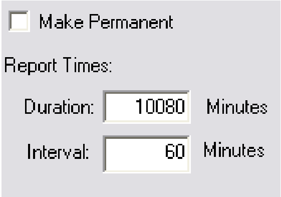
Floppy Drive: Write

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 through the *Report Times* options on the right of the dialog box.



□ Make Permanent

Report Times:

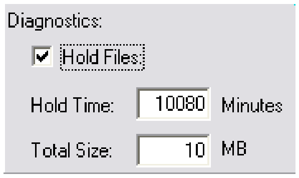
Duration: 10080 Minutes

Interval: 60 Minutes

Select 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, select 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.



Diagnostics:

☑ Hold Files:

Hold Time: 10080 Minutes

Total Size: 10 MB

20.2 Windows Vista/7 Security Client Diagnostic Tools

The following sections explain the diagnostic tools available in the Windows Vista/7 version of the Security Client:

- Section 20.2.1, “Creating a Diagnostics Package,” on page 129
- Section 20.2.2, “Administrator Views,” on page 131
- Section 20.2.3, “Module List,” on page 134
- Section 20.2.4, “Logging,” on page 135

20.2.1 Creating a Diagnostics Package

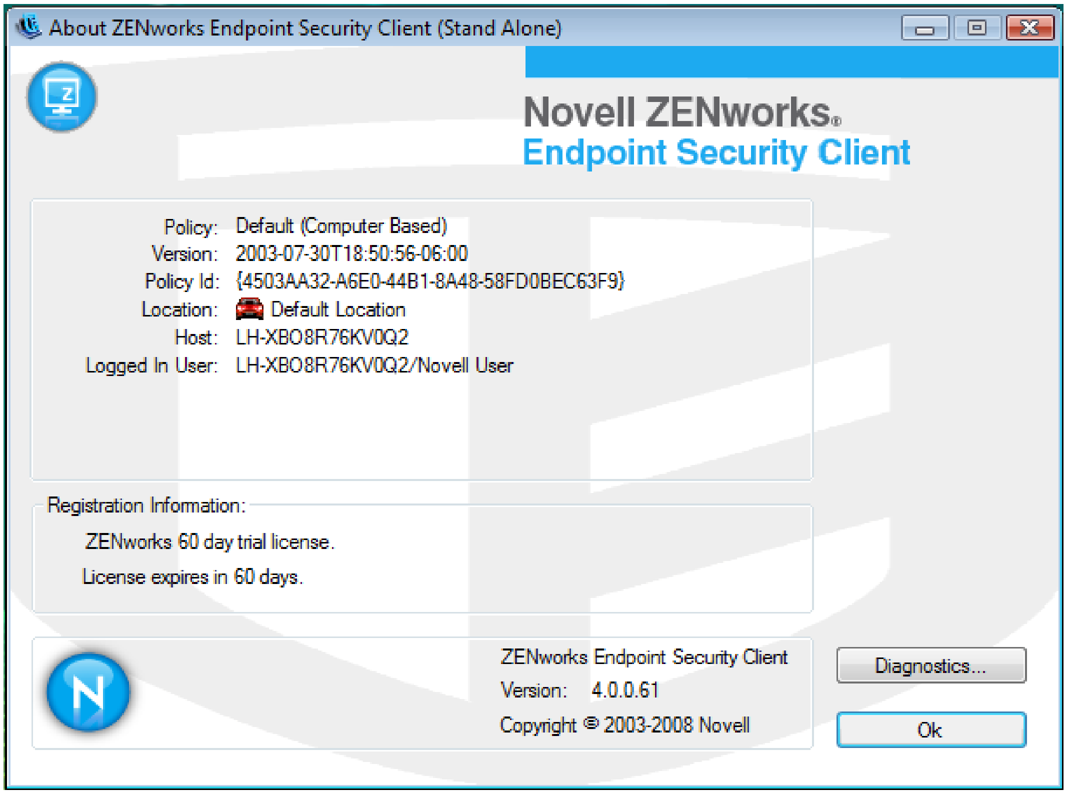
If problems occur because of the Security Client’s presence on the endpoint device, administrators can provide detailed diagnostics information packages to Novell Support. This information is vital in resolution of any issues. The diagnostics package is defined by the following items:

- **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 On the endpoint device, right-click the Security Client icon, then click *About*.



About ZENworks Endpoint Security Client (Stand Alone)

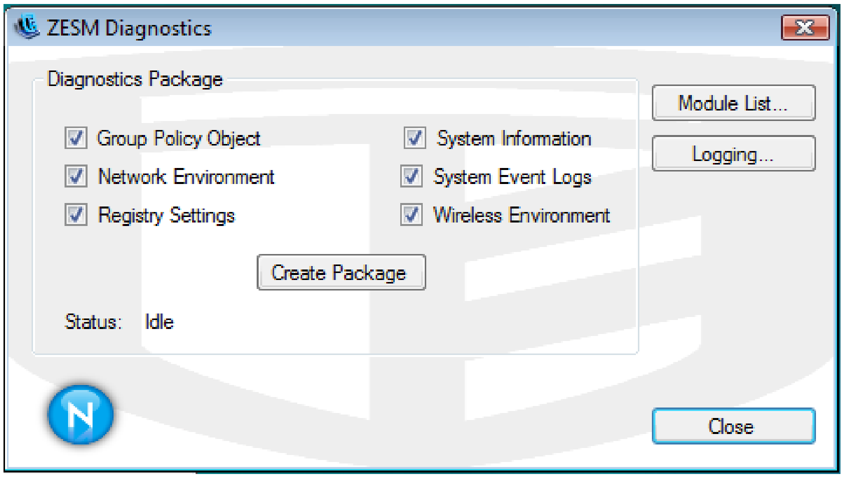
Novell ZENworks®
Endpoint Security Client

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

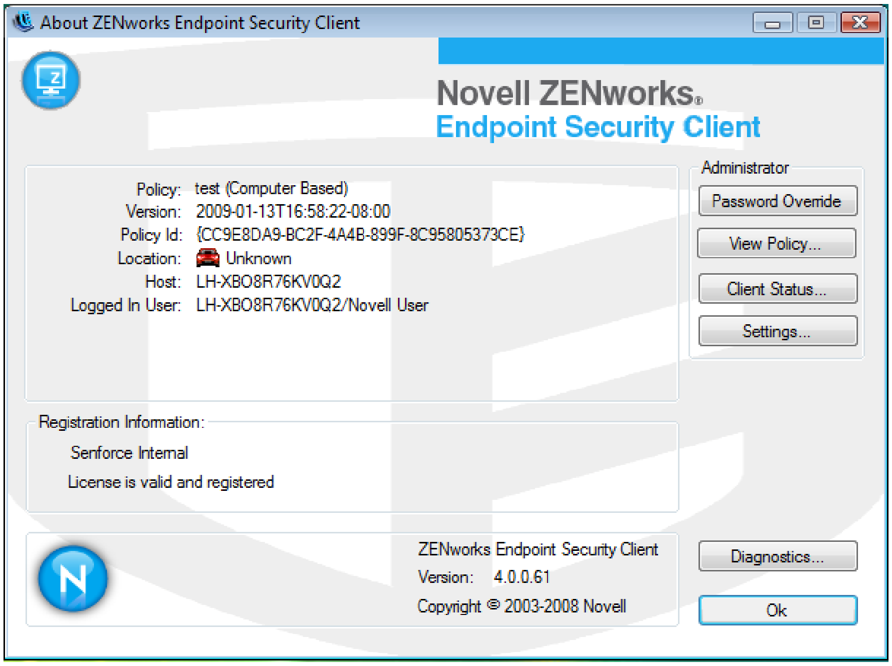
3 Select the items to be included in the package (all are selected by default).

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 Novell Support.

20.2.2 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.



About ZENworks Endpoint Security Client

Novell ZENworks®
Endpoint Security Client

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

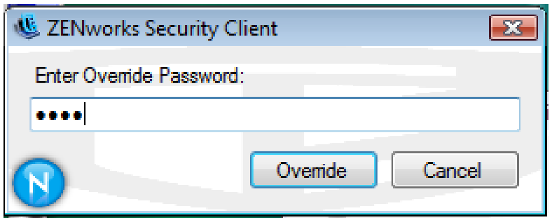
ZENworks Endpoint Security Client
Version: 4.0.0.61
Copyright © 2003-2008 Novell

The following sections contain more information:

- "Password Override" on page 131
- "View Policy" on page 132
- "Client Status" on page 133
- "Settings" on page 133

Password Override

Use the *Password Override* button to temporarily override policy settings by loading an Allow-All policy. Type the password and click *Override*.



ZENworks Security Client

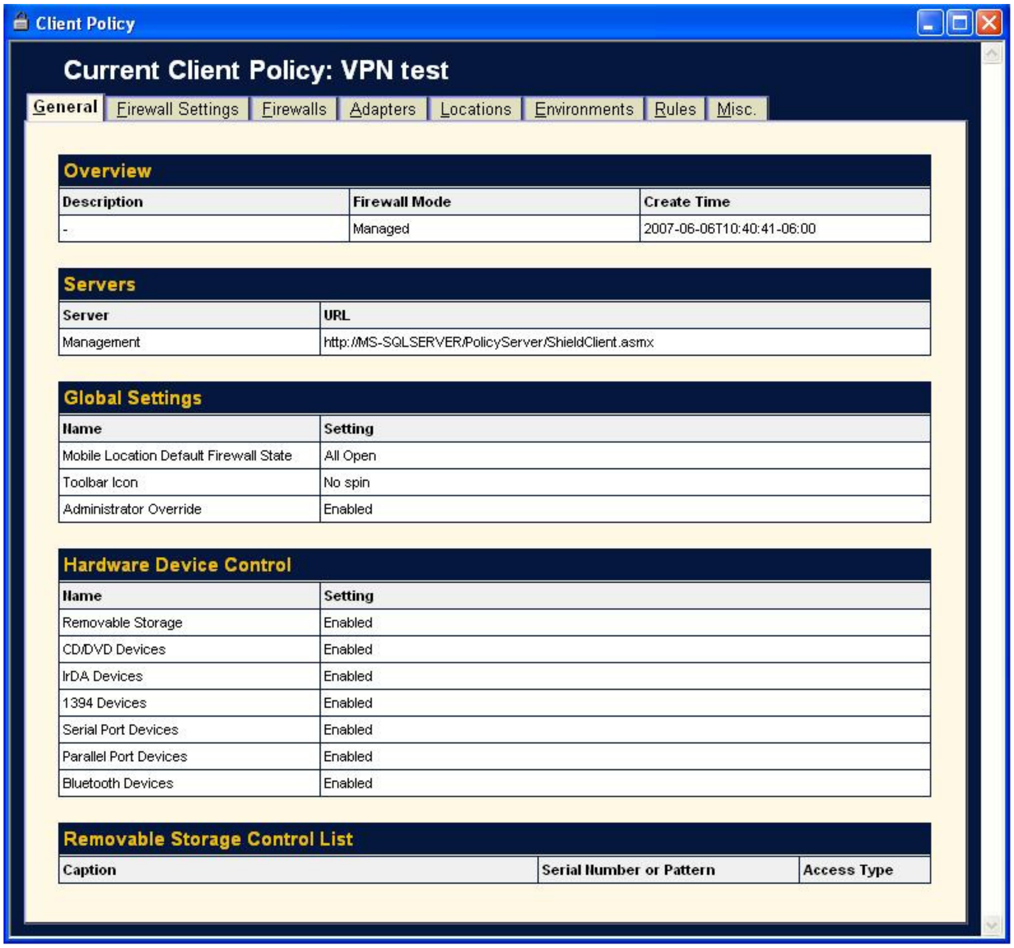
Enter Override Password:
••••

After the password is entered, the *Password Override* button changes to *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.



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

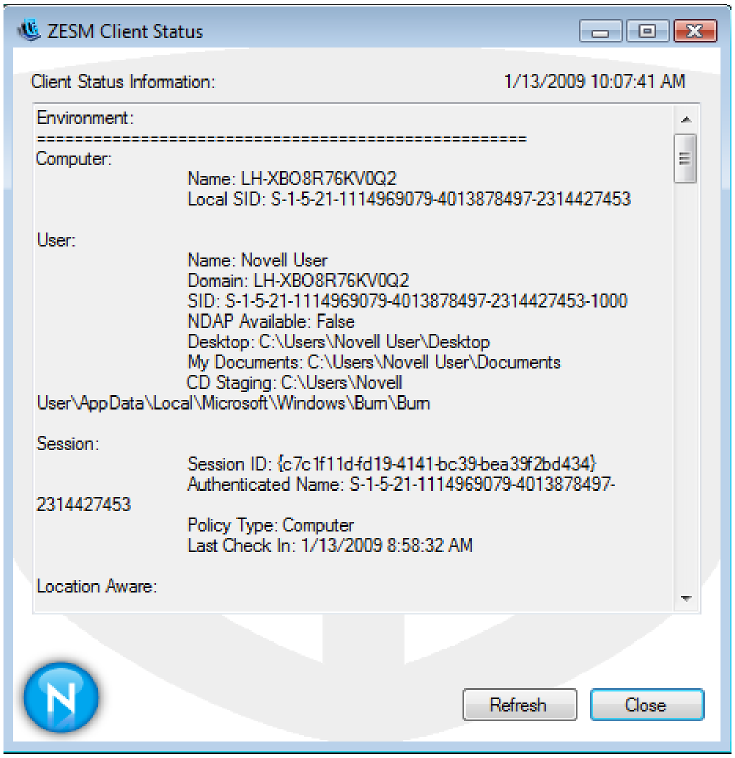
The policy display divides the policy components into the following tabs:

- **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 its settings.
- **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.



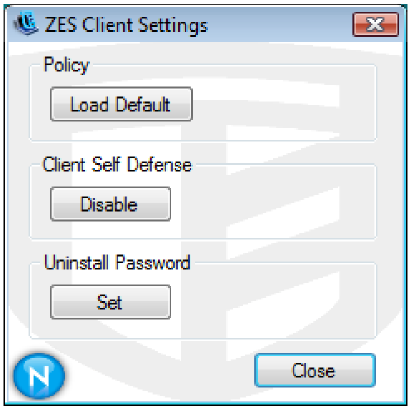
```
Client Status Information:                              1/13/2009 10:07:41 AM

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.



The following sections contain more information:

- "Reset to Default Policy" on page 134
- "Disable Client Self Defense" on page 134
- "Set Uninstall Password" on page 134

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

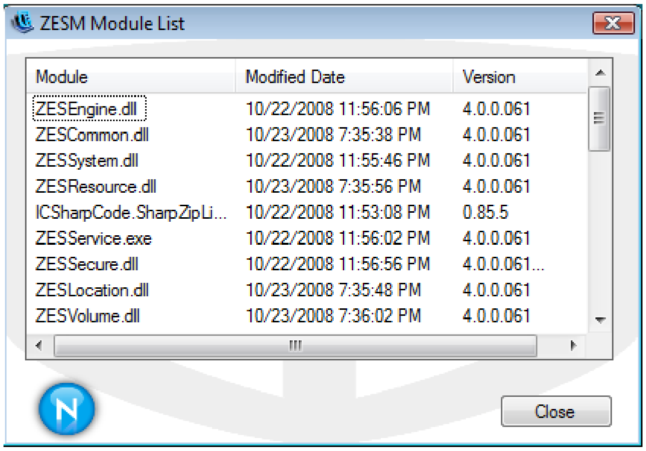
Disables all protections used to keep the client installed and active on the machine.

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.

20.2.3 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 the ZENworks Endpoint Security Client About window, then click *Diagnostics > Module List*.



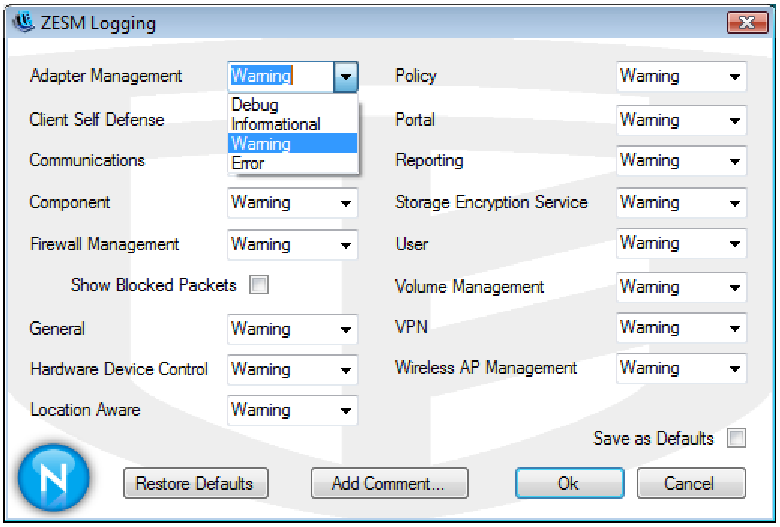
Module	Modified Date	Version
ZESEngine.dll	10/22/2008 11:56:06 PM	4.0.0.061
ZESCommon.dll	10/23/2008 7:35:38 PM	4.0.0.061
ZESSystem.dll	10/22/2008 11:55:46 PM	4.0.0.061
ZESResource.dll	10/23/2008 7:35:56 PM	4.0.0.061
ICSharpCode.SharpZipLi...	10/22/2008 11:53:08 PM	0.85.5
ZESService.exe	10/22/2008 11:56:02 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.

20.2.4 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 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 the ZENworks Endpoint Security Client About window, then click *Diagnostics* > *Logging*.



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.

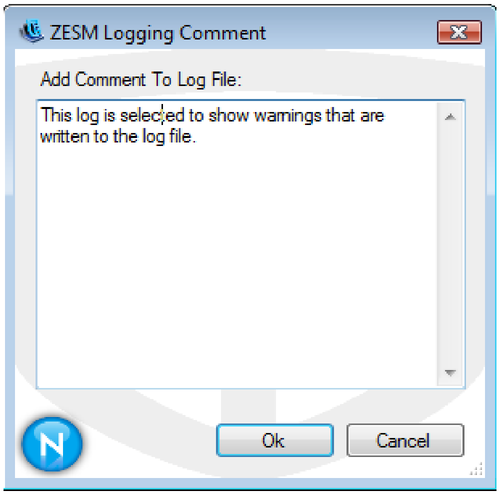
- **Informational:** Records all events when they occur, such as when a network connection event begins and ends.
- **Warning:** Records errors that have occurred but are solvable and do not prevent the client from running.
- **Error:** Records errors that have occurred and prevent the client from running.

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, you should set logging according to the directions of Novell Support and re-create 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.



Add Comment To Log File:

This log is selected to show warnings that are written to the log file.

Auditing

IV

ZENworks® Endpoint Security Management provides both reporting and alerts monitoring to help you monitor and maintain security compliance within your organization.

Generating Standard Reports

21

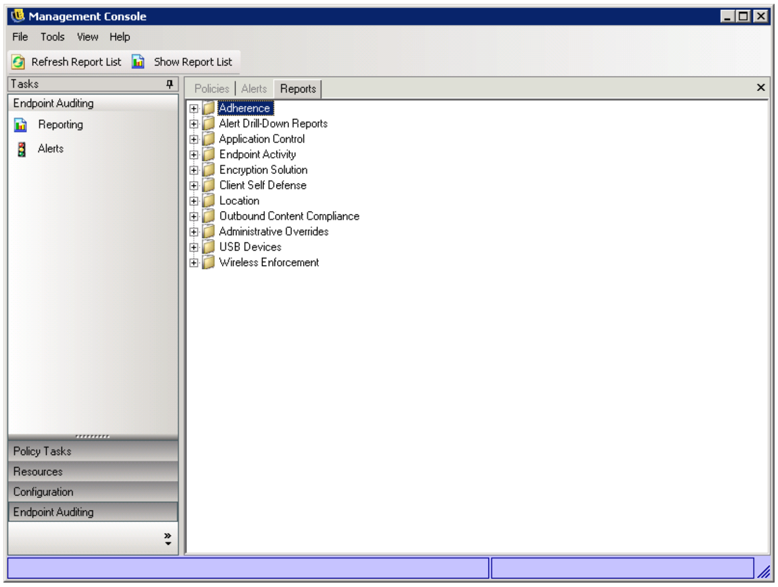
ZENworks® Endpoint Security Management provides a variety of standard reports. The following sections explain how to generate a standard report and provide details about each report.

- Section 21.1, "Generating a Report," on page 139
- Section 21.2, "Adherence Reports," on page 141
- Section 21.3, "Alert Drill-Down Reports," on page 142
- Section 21.4, "Application Control Reports," on page 142
- Section 21.5, "Endpoint Activity Reports," on page 143
- Section 21.6, "Encryption Solutions Reports," on page 144
- Section 21.7, "Client Self Defense Reports," on page 144
- Section 21.8, "Location Reports," on page 144
- Section 21.9, "Outbound Content Compliance Reports," on page 145
- Section 21.10, "Administrative Overrides Reports," on page 145
- Section 21.11, "USB Devices Reports," on page 146
- Section 21.12, "Wireless Enforcement Reports," on page 146

21.1 Generating a Report

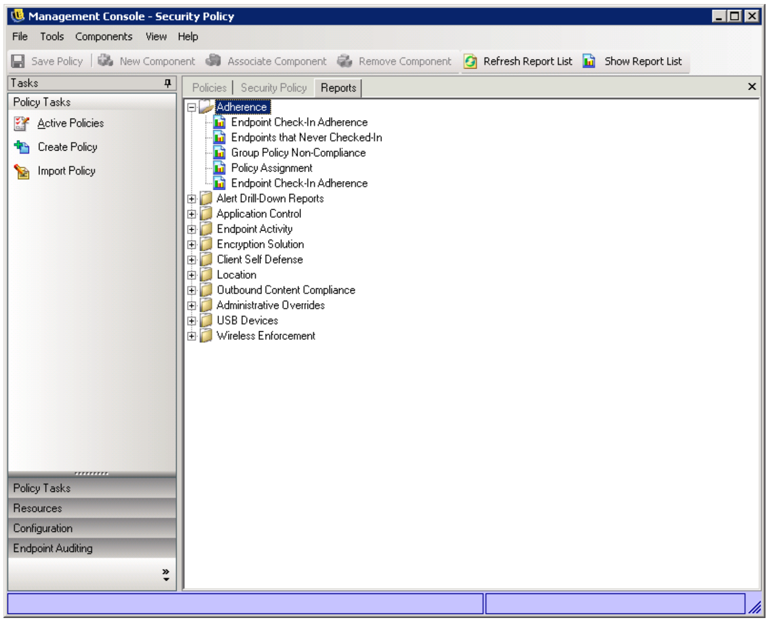
Reports are not available until data has been uploaded from the Security Clients. By default, the data is uploaded every 12 hours. This means that reporting and alerts data is not ready until 12 hours have passed from installation. To adjust this time frame, open the Configuration tool (see "Configuring Data Synchronization Schedules" on page 25), and adjust the Client Reporting time to the number of minutes appropriate for your needs and your environment.

1 Click the *View* menu, then click *Reporting* to display the *Reports* tab.



2 Expand a folder, then select the report you want to generate.

The Management Console displays a description of the report at the bottom of the Reports page. In addition, a *Configure* button is displayed if the report requires configuration before being generated. If configuration is not required, a *Preview* button is displayed. If there is no data available for the report, the button is dimmed.



3 Click *Preview* to generate the report.

or

Click *Configure*, set the configuration options, then click *View* to generate the report.

After the report is generated, you can use the Report toolbar to view, save, and print the report.

- Save the report as a PDF file, Excel* spreadsheet, Word document, or RTF file.
- Print the full report.
- Display or close the parameters list next to the report. Select any of these parameters to drill into the report.
- 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.
- Search for text in the report.
- Zoom in or out.

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.

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

21.2 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:

- Section 21.2.1, “Endpoint Check-In Adherence,” on page 141
- Section 21.2.2, “Endpoints that Never Checked-In,” on page 141
- Section 21.2.3, “Group Policy Non-Compliance,” on page 141
- Section 21.2.4, “Policy Assignment,” on page 141
- Section 21.2.5, “Endpoint Check-In Adherence,” on page 141

21.2.1 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.

21.2.2 Endpoints that Never Checked-In

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

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

21.2.3 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.

21.2.4 Policy Assignment

Lists the users, machines, and group that have received the specified policy. Select the desired policy from the list and click *View* to run the report.

21.2.5 Endpoint Check-In Adherence

Lists the users and machines to which the correct policy is applied.

21.3 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:

- Section 21.3.1, "Client Tampering Alert Data," on page 142
- Section 21.3.2, "Files Copied Alert Data," on page 142
- Section 21.3.3, "Override Attempts Alert Data," on page 142
- Section 21.3.4, "Port Scan Alert Data," on page 142
- Section 21.3.5, "Uninstall Attempt Alert Data," on page 142
- Section 21.3.6, "Unsecure Access Point Alert Data," on page 142

21.3.1 Client Tampering Alert Data

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

21.3.2 Files Copied Alert Data

Lists accounts that have copied data to removable storage.

21.3.3 Override Attempts Alert Data

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

21.3.4 Port Scan Alert Data

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

21.3.5 Uninstall Attempt Alert Data

Lists users who have attempted to uninstall the Security Client.

21.3.6 Unsecure Access Point Alert Data

Lists unsecured access points detected by the Security Client.

21.4 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 *Application Control Reports* to expand the list to display the following report:

- Section 21.4.1, “Application Control Details,” on page 143

21.4.1 Application Control Details

Lists the date, location, the action taken by the 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.

21.5 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:

- Section 21.5.1, “Blocked Packets by IP Address,” on page 143
- Section 21.5.2, “Blocked Packets by User,” on page 143
- Section 21.5.3, “Network Usage Statistics by User,” on page 143
- Section 21.5.4, “Network Usage Statistics by Adapter Type,” on page 143

21.5.1 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.

21.5.2 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.

21.5.3 Network Usage Statistics by User

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

21.5.4 Network Usage Statistics by Adapter Type

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

21.6 Encryption Solutions Reports

When endpoint encryption is activated, the transfer 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:

- Section 21.6.1, "File Encryption Activity," on page 144
- Section 21.6.2, "Encryption Exceptions," on page 144

21.6.1 File Encryption Activity

Lists files that have had encryption applied.

21.6.2 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).

21.7 Client Self Defense Reports

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

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

- Section 21.7.1, "Endpoint Security Client Hack Attempts," on page 144

21.7.1 Endpoint Security Client Hack Attempts

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

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

21.8 Location Reports

Provides data for the locations that are most commonly used by users.

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

- Section 21.8.1, "Location Usage Data by Date and User," on page 144

21.8.1 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.

21.9 Outbound Content Compliance Reports

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

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

- Section 21.9.1, “Removable Storage Activity by Account,” on page 145
- Section 21.9.2, “Removable Storage Activity by Device,” on page 145
- Section 21.9.3, “Detected Removable Storage Devices,” on page 145
- Section 21.9.4, “Chart 7 Days of Removable Storage Activity by Account,” on page 145

21.9.1 Removable Storage Activity by Account

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

21.9.2 Removable Storage Activity by Device

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

21.9.3 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.

21.9.4 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.

21.10 Administrative Overrides Reports

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

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

- Section 21.10.1, “Security Client Overrides,” on page 145

21.10.1 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.

21.11 USB Devices Reports

Shows a Security Client inventory of USB devices 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.

21.12 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:

- Section 21.12.1, "Wireless Connection Availability," on page 146
- Section 21.12.2, "Wireless Environment History," on page 146

21.12.1 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.

21.12.2 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.

Generating Custom Reports

22

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

The following sections contain more information:

22.1 Software Requirements

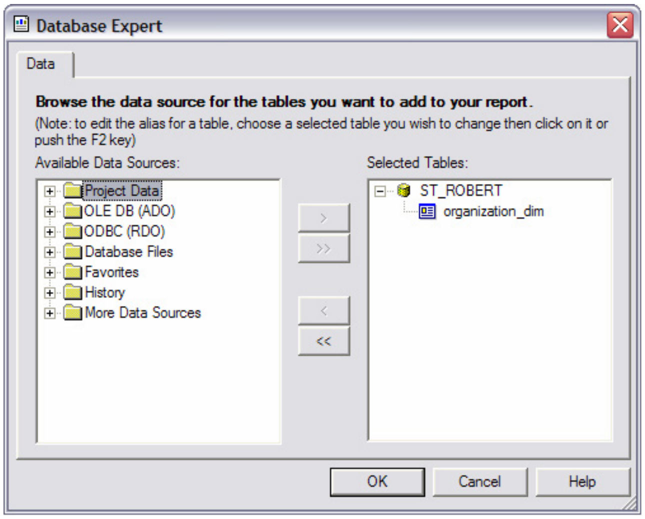
You can use ODBC-compliant reporting tools (for example, Crystal Reports* and Actuate*) to create custom reports that are not included in the list of standard reports. These reporting tools can view and query the reporting information from a common data warehouse.

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).

22.2 Creating a ZENworks Endpoint Security Management Compliant Report

Every custom report to be integrated into the system has the following requirements:

- 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.



Database Expert

Data

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)

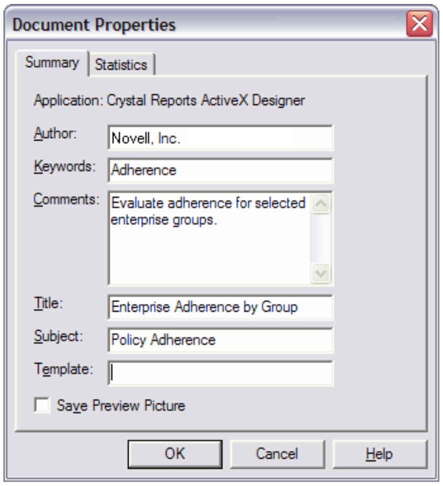
Available Data Sources:

- Project Data
- OLE DB (ADO)
- ODBC (RDO)
- Database Files
- Favorites
- History
- More Data Sources

Selected Tables:

- ST_ROBERT
  - organization_dim

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



Document Properties

Summary | Statistics

Application: Crystal Reports ActiveX Designer

Author: Novell, Inc.

Keywords: Adherence

Comments: Evaluate adherence for selected enterprise groups.

Title: Enterprise Adherence by Group

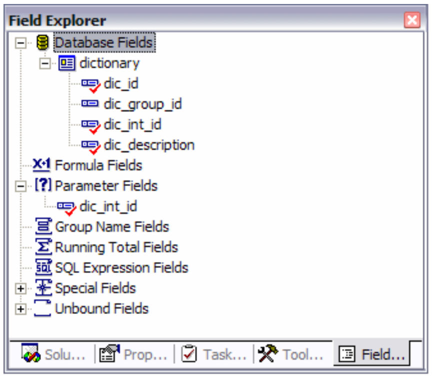
Subject: Policy Adherence

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.



22.3 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 defines 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. 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. Specify the Management Service server as the server.
4. Specify the SQL account name and password.
5. Specify the Reporting Service database name (default name is STRSDB) as the database.

The following views are available for report generation:

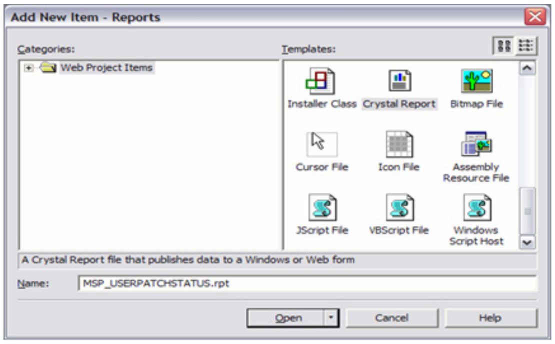
- **EVENT_ACCESSPOINT_FACT_VW:** Describes the access points observed by user, day, policy, location, and access point instance.
- **EVENT_BLOCKEDPACKETS_FACT_VW:** Describes the summarized instances of port activity that was blocked due to policy configuration by the endpoint. The information included is logged user, day, policy, location, and source/destination IP/port.
- **EVENT_CLIENTACTIVITY_FACT_VW:** 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:** Describes the summarized instances of application use (duration) by user, day, policy, location and application.
- **EVENT_CLIENTDEFENSE_HACK_FACT_VW:** 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:** 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:** 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:** 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:** 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:** 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:** Describes the time at location as well as the adapter (configuration and type) used at the location. The data is grouped by user, day, policy, and location.
- **EVENT_CLIENTRULE_FACT_VW:** 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:** 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:** Describes when a component has been created or edited. The data is grouped by user, day, component, and action.
- **EVENT_ORGANIZATIONACTION_FACT_VW:** 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:** 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:** Describes the policy and component assignment to an organization.
- **EVENT_SERVERACTION_FACT_VW:** Describes the user activity with the Distribution Service (for example, Check In).
- **EVENT_USERACTION_FACT_VW:** Describes the user policy activity with the Distribution Service (Policy, Key, EFS Key, Schema downloads).

22.4 Creating a Report

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

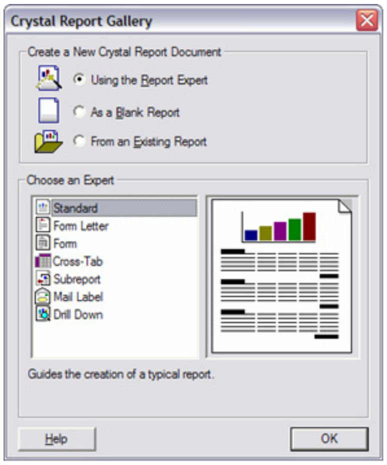
1 From the IDE, select *Add New Item* and add a new Crystal Report.



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

Name: MSP_USERPATCHSTATUS.rpt

2 Create a report using the wizard.

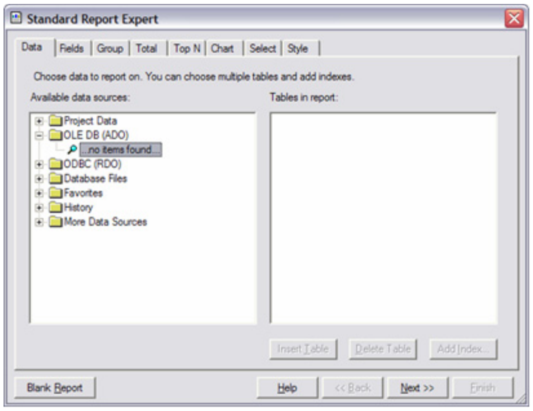


● Using the Report Expert
○ As a Blank Report
○ From an Existing Report

Standard

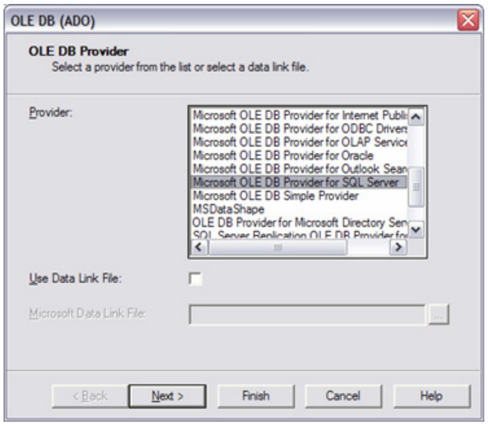
Guides the creation of a typical report.

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



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

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*.



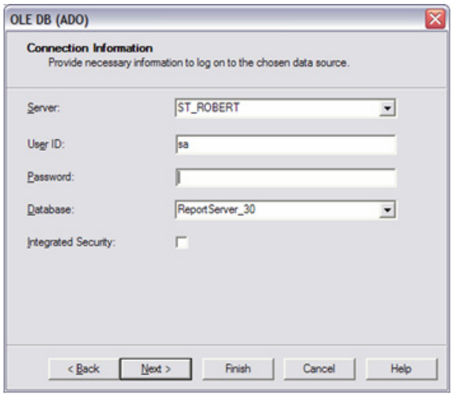
OLE DB (ADO)
OLE DB Provider
Provider:
Microsoft OLE DB Provider for Internet Publi
Microsoft OLE DB Provider for ODBC Drivers
Microsoft OLE DB Provider for OLAP Service
Microsoft OLE DB Provider for Oracle
Microsoft OLE DB Provider for Outlook Sear
Microsoft OLE DB Provider for SQL Server
Microsoft OLE DB Simple Provider
MSDataShape
OLE DB Provider for Microsoft Directory Ser
SQL Server Replication OLE DB Provider fo
Use Data Link File:
Microsoft Data Link File:
< Back
Next >
Finish
Cancel
Help

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

Provider: Microsoft OLE DB Provider for SQL Server

Use 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 4.1 Installation Guide* for more information). Click *Next,* then click *Finish*.



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

Server: ST_ROBERT

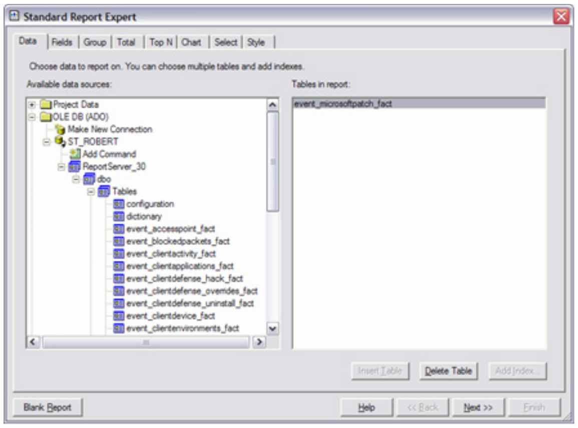
User ID: sa

Password:

Database: ReportServer_30

Integrated Security: □

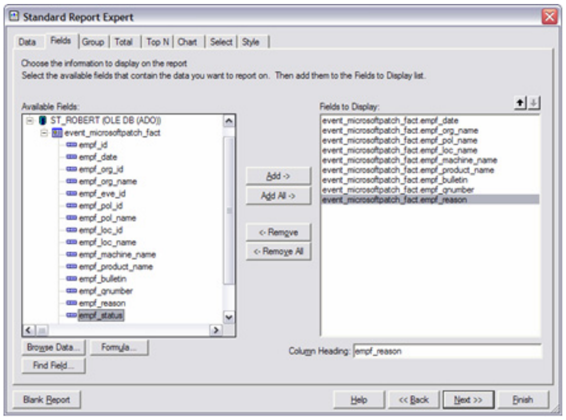
6 Select the desired source table or view for your report by expanding the tree nodes as shown below.



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

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.

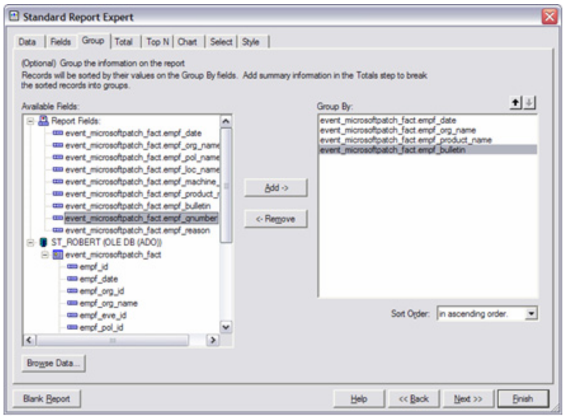


Choose the information to display on the report
Select the available fields that contain the data you want to report on. Then add them to the Fields to Display list.

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_gnumber
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.

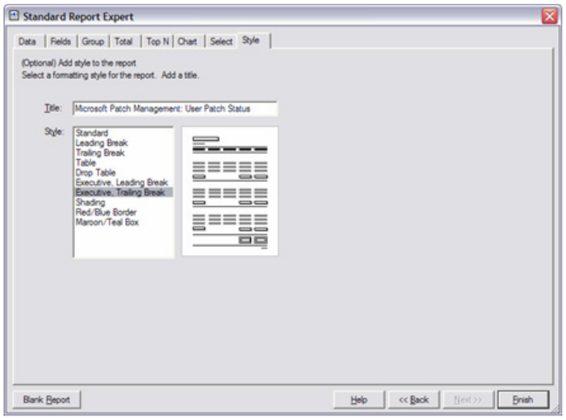

Standard Report Expert
Data
Fields
Group
Total
Top N
Chart
Select
Style
Available Fields:
Report Fields:
event_microsoftpatch_fact.empf_date
event_microsoftpatch_fact.empf_org_name
event_microsoftpatch_fact.empf_pol_name
event_microsoftpatch_fact.empf_loc_name
event_microsoftpatch_fact.empf_machine_
event_microsoftpatch_fact.empf_product_r
event_microsoftpatch_fact.empf_bulletin
event_microsoftpatch_fact.empf_gnumber
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
Add ->
<- Remove
Browse Data...
Blank Report
Help
<< Back
Next >>
Finish

(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.

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.

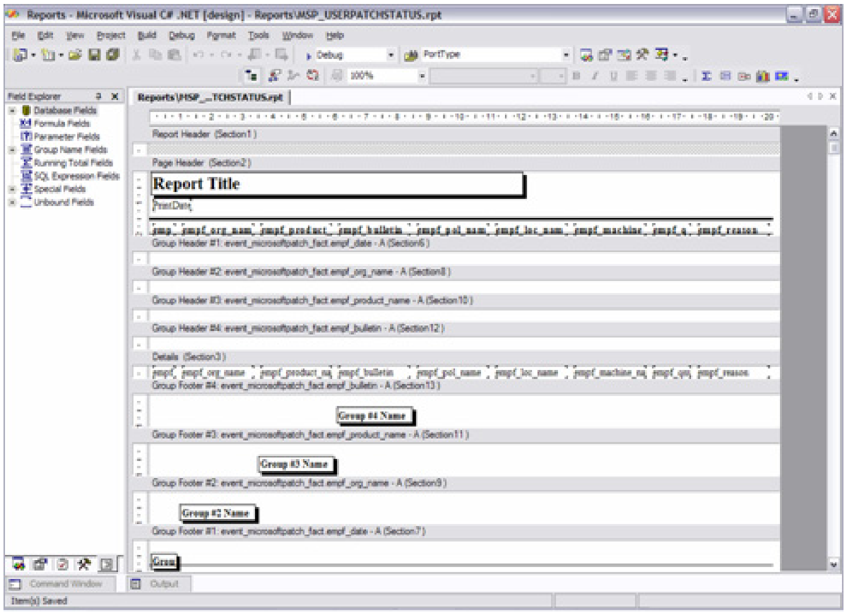

Standard Report Expert

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

Title: Microsoft Patch Management: User Patch Status

Style: Executive, Trailing Break

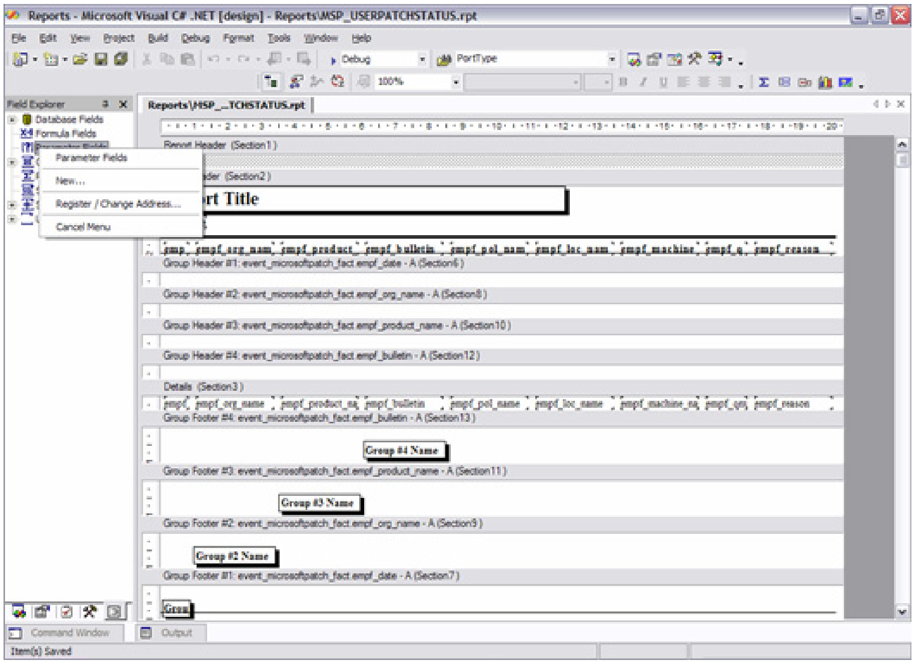
The Report Builder displays.


Reports - Microsoft Visual C# .NET [design] - Reports\MSP_USERPATCHSTATUS.rpt

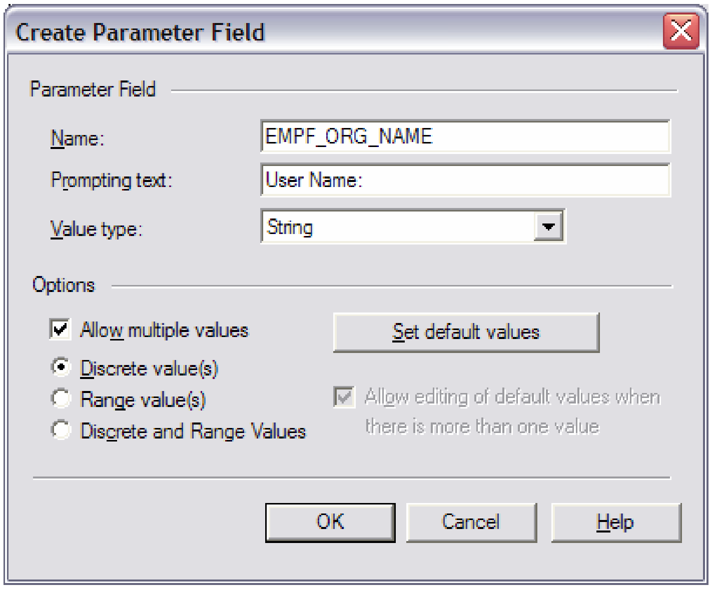
Reports\MSP_...TCHSTATUS.rpt

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
File Edit View Project Build Debug Format Tools Window Help
Debug
PortType
100%
Field Explorer
Database Fields
Formula Fields
Parameter Fields
New...
Register / Change Address...
Cancel Menu
Reports\MSP_...TCHSTATUS.rpt
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)
Command Window
Output
Item(s) Saved

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

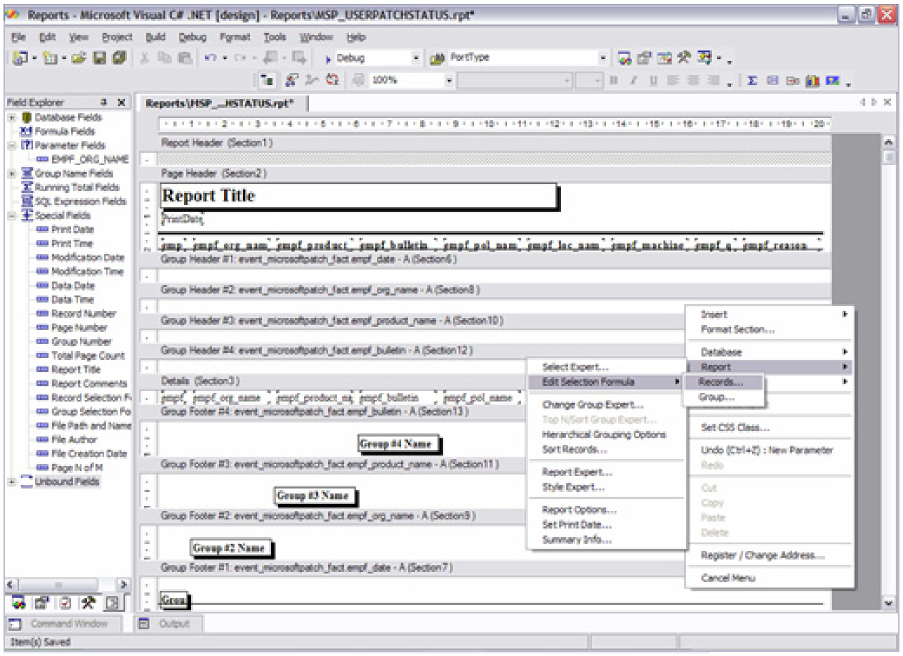
● Discrete value(s)

○ Range value(s)

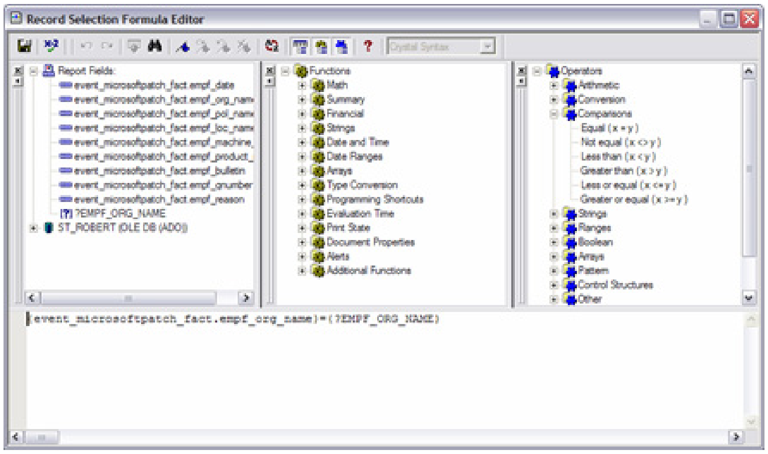
○ Discrete and Range Values

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

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


Reports - Microsoft Visual C# .NET [design] - Reports\MSP_USERPATCHSTATUS.rpt*
File Edit View Project Build Debug Format Tools Window Help
Field Explorer
Database Fields
Formula Fields
Parameter Fields
EMPF_ORG_NAME
Group Name Fields
Running Total Fields
SQL Expression Fields
Special Fields
Print Date
Print Time
Modification Date
Modification Time
Data Date
Data Time
Record Number
Page Number
Group Number
Total Page Count
Report Title
Report Comments
Record Selection F
Group Selection Fo
File Path and Name
File Author
File Creation Date
Page N of M
Unbound Fields
Reports\MSP_...HSTATUS.rpt*
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...
Top N/Sort 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
Command Window
Output
Item(s) Saved

13 Using the new parameter, specify only the records where the field equals the values selected in the parameter. Select the column, select a comparison (=), and then select 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 saved into the `\Program Files\Novell\ESM Management Console\Reports\Reports\` directory on the Management Console machine. The new report displays in the reports list in the Reports tab of the Management Console (click *Refresh List* to display the new reports).

Using Alerts Monitoring

23

Alerts monitoring allows you to 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.

Alerts monitoring is available for the following areas:

- **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 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 23.1, "Configuring Endpoint Security Management for Alerts," on page 157
- Section 23.2, "Configuring Alert Triggers," on page 158
- Section 23.3, "Managing Alerts," on page 159

23.1 Configuring Endpoint Security Management for Alerts

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

The following sections contain more information:

- Section 23.1.1, "Activating Reporting," on page 157
- Section 23.1.2, "Optimizing Synchronization," on page 158

23.1.1 Activating Reporting

Reporting should be activated in each security policy. See Chapter 13, "Configuring a Policy's Compliance Reporting," on page 97 for details on setting up reporting for a security policy. Adjust report send times to an interval that gives you consistent updates on endpoint status. Additionally, an alert cannot activate without a report. Any activity you want to be alerted to must have an appropriate report assigned to it in the security policy.

23.1.2 Optimizing Synchronization

By default, the ZENworks Endpoint Security Management Reporting Service synchronizes 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 "Configuring Data Synchronization Schedules" on page 25) and adjust the Client Reporting time to the number of minutes appropriate for your needs and your environment.

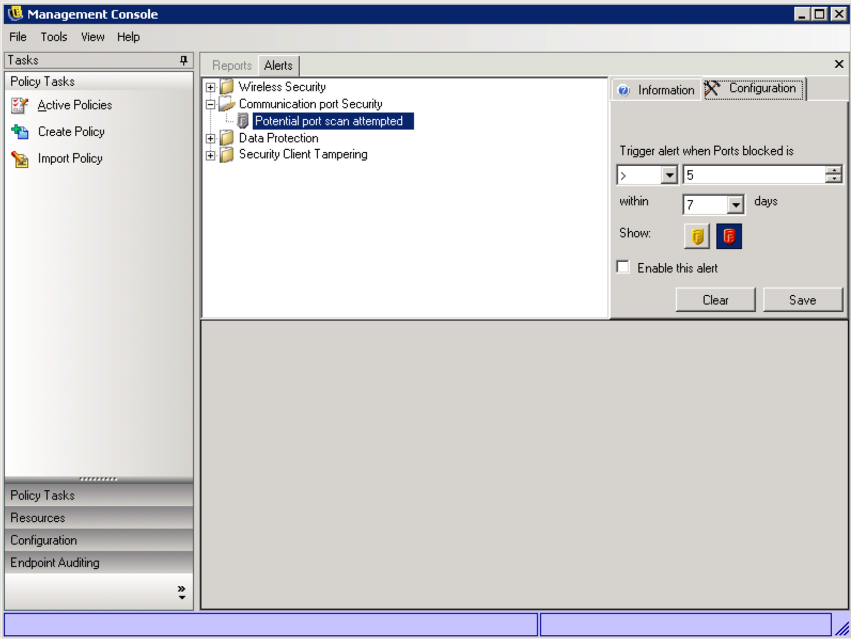
When data is needed immediately, the Service Synchronization option in the Configuration tool immediately synchronizes the Policy Distribution Service (which collects the reporting data from the endpoints) and the Reporting Service, which updates all alerts based on the newly collected data. See Chapter 4, "Forcing Data Synchronization," on page 27 for details.

23.2 Configuring Alert Triggers

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

To adjust alerts from their defaults:

1 In the Management Console, click the *View* menu, then click *Alerts* to display the *Alerts* tab.



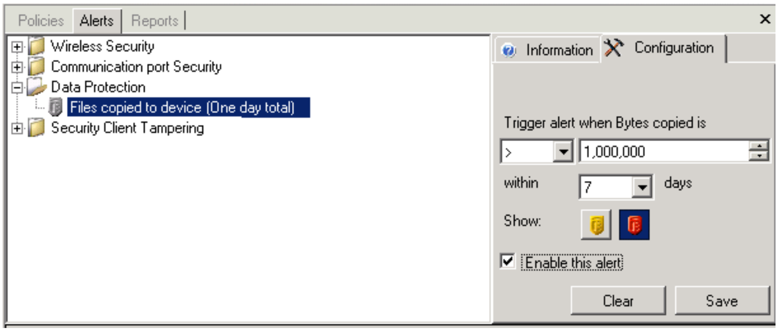
Trigger alert when Ports blocked is > 5

within 7 days

Show:

□ Enable this alert

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



- Wireless Security
- Communication port Security
- Data Protection
  - Files copied to device (One day total)
- Security Client Tampering

Trigger alert when Bytes copied is

> 1,000,000

within 7 days

Show:

☑ Enable this alert

3 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 (>=)

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

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

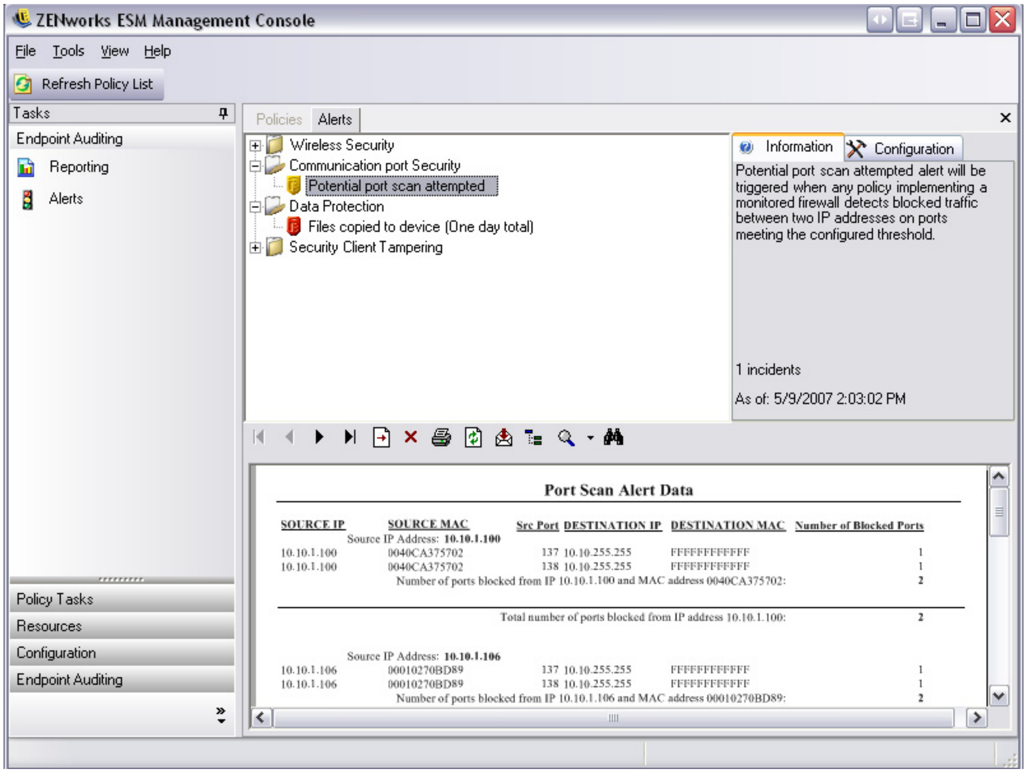
6 Select the trigger type, whether it's the warning icon or the emergency icon .

7 Click *Enable this alert*.

8 Click *Save*.

23.3 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 basis for individuals or groups. To help identify the issue, Alert reports are displayed when the alert is selected.



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

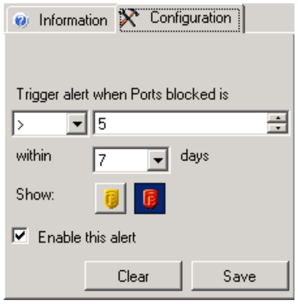
```
                                 Port Scan Alert Data

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, and shows 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 clicking *Reporting*.

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

To clear an alert:

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.

The data is still available in the reporting database. The alert does not reactivate until new data is received.

Utilities

V

ZENworks® Endpoint Security Management includes the following administrative utilities:

ZENworks File Decryption Utility

24

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 an 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 24.1, "Using the File Decryption Utility," on page 163
- Section 24.2, "Using the Administrator Configured Decryption Utility," on page 163

24.1 Using the File Decryption Utility

1. Plug the storage device into the appropriate port on the endpoint device.
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.

24.2 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 because it can potentially compromise all current keys used by the ZENworks Storage Encryption Solution. However, if the data is otherwise unrecoverable, this configuration might 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` (for 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.

Override-Password Key Generator 25

Productivity interruptions that a user might experience due to restrictions to connectivity, disabled software execution, or access to removable storage devices are probably caused by the security policy the Security Client is enforcing. Changing locations or firewall settings usually lifts these restrictions and restores the interrupted functionality. However, in some cases the restriction might affect all locations and firewall settings, or the user might be 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 a password-protected override for specified users and functionality, which temporarily permits the necessary activities.

Password overrides disable the current security policy and restores the default All Open policy for a predefined period of time. After the time-limit expires, or if the endpoint reboots, the current policy is restored. The password for a policy is set in the security policy's Global settings.

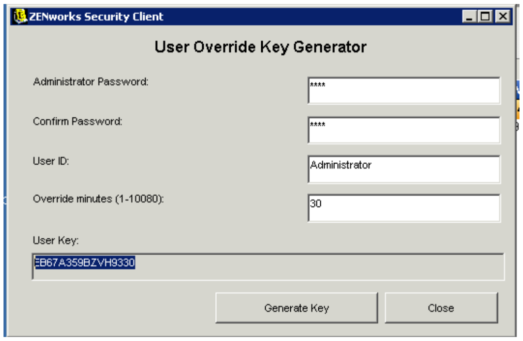
Password override does the following:

- Overrides application blocking
- Allows users to change locations
- Allows users to change firewall settings
- Overrides hardware control (thumb drivers, CD ROM, etc.)

The password in a policy should never be issued to an end user. You should use the Override-Password Key Generator to generate a key for short-term use.

To generate an override key:

1 On the Management Console machine, click *Start* > *All Programs* > *Novell* > *ESM Management* > *Override-Password Generator*.



Administrator Password: ****

Confirm Password: ****

User ID: Administrator

Override minutes (1-10080): 30

User Key: EB67A359BZVH9330

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.

6 Copy the key and give it to the end user.

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. For detailed instructions, see "Password Override" in the *ZENworks Endpoint Security Client for Windows 2000/XP User Guide* or "Password Override" in the *ZENworks Endpoint Security Client for Windows Vista/7 User Guide*.

This key is valid for that user's policy only and only for the specified amount of time or until the computer reboots. Once the key has been used or the computer reboots, the key cannot be used again.

If you publish a new policy to fix the problems with the user's current policy, you should instruct the user to check for a policy update. For instructions, see "Policy Updates" in the *ZENworks Endpoint Security Client for Windows 2000/XP User Guide* or "Policy Updates" in the *ZENworks Endpoint Security Client for Windows Vista/7 User Guide*.

Device Scanner

26

The Device Scanner collects data about the USB devices connected to a computer. This includes removable storage devices, printers, mice, keyboards, and other types of USB devices.

After you collect device data, you can review the data and make modifications as necessary. The device data can then be imported into the Management Console for use during creation of Storage Device Control policies.

For information about using the Device Scanner to scan a device, see the *ZENworks Endpoint Security Management 4.1 Device Scanner Guide*.

For information about importing device data into the Preferred Device list of a Storage Device Control policy, see Section 10.5, “Storage Device Control,” on page 47

Appendixes

VI

Predefined TCP/UDP Port Groups

A

The following TCP/UDP port groups are included as predefined groups:

Name	Description	Transport	Value
All Ports	All Ports	All	1-65535
BlueRidge VPN	Ports used by the Blue Ridge 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
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

Name	Description	Transport	Value
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

Predefined Access Control Lists

B

There are two ways you can use the predefined Access Control Lists:

- When you add an Access Control List, you can select the predefined ACL from the list of shared components. In this case, you would use the Component Name referenced in the table below.
- When you edit an existing Access Control List, you can add the Macro Name to the IP/MAC Address field.

For more information about using the predefined Access Control Lists, see "Access Control Lists" on page 73.

Component Name	Macro Name	Description
ARP	[Arp]	Allows 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 by 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 provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.
ICMP	[Icmp]	Allows 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.
IP Multicast	[IpMulticast]	Allows 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 can be distributed by using either IP or Ethernet addresses.
Ethernet Multicast	[EthernetMulticast]	Allows Ethernet multicast packets.

Component Name	Macro Name	Description
IP Subnet Broadcast	[IpSubnetBrdcast]	Allows 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 Server	[Snap]	Allows Snap encoded packets.
Logical Link Layer Control	[LLC]	Allows LLC encoded packets.
802.1x	[Allow8021X]	Allows 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 that uses the 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.
Default Gateway	[Gateway]	Represents the current IP configuration default gateway address. When this value is entered, the Security Client allows all network traffic from the current IP configuration default gateway as a trusted ACL.
All Gateways	[GatewayAll]	Same as [Gateway] but for all defined gateways.
Default Wins	[Wins]	Represents the current client IP configuration default WINS server address. When this value is entered, the Security Client allows all network traffic from the current IP configuration default WINS server as a trusted ACL.
All Wins	[WinsAll]	Same as [Wins] but for all defined WINS servers.
Default Dns	[Dns]	Represents the current client IP configuration default DNS server address. When this value is entered, the Security Client allows all network traffic from the current IP configuration default DNS server as a trusted ACL.
All Dns	[DnsAll]	Same as [Dns] but for all defined DNS servers.
Default Dhcp	[Dhcp]	Represents current client IP configuration Default DHCP server address. When this value is entered, the Security Client allows all network traffic from the current IP configuration default DHCP server as a trusted ACL.
All Dhcp	[DhcpAll]	Same as [Dhcp] but for all defined DHCP servers.

Predefined Application Controls

C

The following is a list of predefined Application Controls. The default execution behavior for each control is *No Execution*.

Name	Applications
Known Malware	1000+ applications
P2P Software	50+ applications
Instant Messaging	`aim.exe`; `icq.exe`; `msmsgs.exe`; `msnmsgr.exe`; `trillian.exe`; `ypager.exe`
Internet Media	`mplayer2.exe`; `wmplayer.exe`; `naplayer.exe`; `realplay.exe`; `spinner.exe`; `QuickTimePlayer.exe`
Web Browsers	`iexplore.exe`; `netscape.exe`; `netscp.exe`; `firefox.exe`

Advanced Scripting Rules

D

The following sections provide information to help you create scripts for use in a security policy's Integrity and Remediation rules (see Chapter 12, "Configuring a Policy's Integrity and Remediation Rules," on page 87).

D.1 Supported Script Languages

ZENworks® Endpoint Security Management supports standard JScript and VBScript coding methods, with the following exceptions:

1. WScript.Echo is not supported because return values can't be sent back to a parent window that 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
```

D.2 Rule Scripting

A rule consists of two parts. The first part is the trigger events that determine when to execute the rule. The second part is the scripting code that contains the logic of the rule. The 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:

- **Query:** Provides methods to get the current state of the client. For example, information about the adapters, shield states, and location.
- **Action:** Provides methods that get the client to do something. For example, a call that puts the client into a quarantined shield state.
- **Storage:** 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:

- **IClientAdapter:** Describes an adapter in the client network environment.
- **IClientEnvData:** Returns environment data about a server or wireless access point.
- **IClientNetEnv:** Provides network environment information.
- **IClientWAP:** Provides information about a wireless access point.
- **IClientAdapterList:** Lists the adapters in the client network environment.

D.3 Trigger Events

Triggers are events that cause the 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

  Description: Adapter arrival has occurred.

  Parameters: None.
- AdapterRemoval

  Description: Adapter had been removed.

  Parameters: None.
- DownloadFailed

  Description: This event is triggered in response to Action.DownloadAsync if the file was not successfully downloaded.

  Parameters: None.
- DownloadSuccess

  Description: This event is triggered in response to Action.DownloadAsync if the file was successfully downloaded

  Parameters: None.
- LocationChange

  Description: 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 the location.

- MediaConnect

  Description: The adapter has a connection.

  Parameters: None.

- MediaDisconnect

  Description: The adapter has lost its connection.

  Parameters: None.

- PolicyUpdated

  Description: Called when the Security Client is first started and whenever a new policy is applied.

  Parameters: None.

- ProcessChange

  Description: Triggered whenever a process is created or deleted.

  Parameters: None.

- Startup

  Description: Run the rule when the engine is started.

  Parameters: None.

- TimeOfDay

  Description: Run the rule at a particular time or times of day, or at least once a day. Stores the last trigger time.

  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

  Description: Run the rule every *n* milliseconds.

  Parameters:

Interval:	Number of milliseconds

- UserChangeShield

  Description: The user had manually changed the shield state.

  Parameters: None.

- WithinTime

  Description: Run the rule every *n* minutes starting from the last time the rule was executed. If the computer is turned off it executes the rule if the specified time has passed since the last time the rule was executed.

Parameters:

WithinMinutes:	Number of seconds

D.4 Script Namespaces

- Section D.4.1, "General Enumerations and File Substitutions," on page 180
- Section D.4.2, "Action Namespace," on page 182
- Section D.4.3, "Query Namespace," on page 188
- Section D.4.4, "Storage Namespace," on page 198

D.4.1 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
```

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

D.4.2 Action Namespace

CheckForUpdate

JScript:

```
Action.CheckForUpdate();
```

VBScript:

```
Action.CheckForUpdate()
```

ClearFixedShieldState, SetShieldStateByName, Trace, Sleep

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

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 that can be stamped. This script then switches to location Base, stamps it, sleeps for 20 seconds, makes sure it didn't spin out of the location by switching back to Base, then clears 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

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 creates a Message Box with all parameters and then waits 10 seconds, (during which the tester should click OK to end box display). The script then displays the Message Box by the ID and waits 10 seconds, (again, the tester should click OK to end box display). Finally, it displays the Message Box by name.

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

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 that was launched.

JScript:

```
Action.LaunchAsUserWithCode(appToLaunch, "sParameters", "sWorkingDir", bShow, 
bWait, nExitCode);
```

VBScript:

```
Action.LaunchAsUserWithCode appToLaunch, "sParameters", "sWorkingDir", bShow, 
bWait, nExitCode
```

Details:

Preliminary setup is required by creating a policy that includes a new Integrity rule with a custom message. The custom message includes a launch link that was added to the SCC menu bar.

LaunchLinkByName

When you set 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:

Logging must be enabled as a prerequisite.

Message

An asynchronous message is displayed and the script continues.

JScript:

```
Action.Message("Display sync message");
```

VBScript:

```
Action.Message "Display sync message"
```

A synchronous message is displayed and waits for the user to 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 of the 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"
```

D.4.3 Query Namespace

- "FileExistsVersion" on page 189
- "GetAdapters" on page 189
- "GetCheckinTime" on page 190
- "GetLocationMatchData, LocationMatchCount" on page 190
- "IsAdapterTypeConnected" on page 191
- "IsAuthenticated" on page 192

- "IsWindowsXP" on page 192
- "IsWindows2000" on page 192
- "ProcessIsRunning" on page 192
- "RegistryKeyExists" on page 193
- "RegistryValueDWORD" on page 193
- "RegistryValueExists" on page 193
- "RegistryValueString" on page 194
- "LocationName, LocationUuid, MaxConnectionSpeed, OSServicePack, PolicyName, PolicyTime, PolicyUuid, LocationIsStamped, TriggerEvent, TriggerEventData1" on page 194
- "RemovableMediaState, CDMediaState, HDCState, WiFiDisabledState, WiFiDisabledWhenWiredState, AdHocDisabledState, AdapterBridgeDisabledState, MinimumWiFiSecurityState, DialupDisabledState" on page 195
- "RemovableMediaState, CDMediaState, HDCState, IsWiFiDisabled, IsWiFiDisabledWhenWired, IsAdHocDisabled, IsAdapterBridgeDisabled, MinimumWiFiSecurityState, IsWiredDisabled, IsDialupDisabled" on page 197

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.

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 gets a list of adapters, the length of the list (number of adapters), and enumerates 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 network environment to be defined for a location in the policy in order to provide useful data. This script then gets the Location Match Count and if the count is greater than 0, it enumerates 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)
```

D.4.4 Storage Namespace

There are two kinds of storage in the Security Client storage space. Persistent storage remains between sessions of the client, but transient storage exists only for the duration of the session. Transient values can be accessed in each rule script invocation. Also, persistent storage can only store and retrieve string values, and transient storage stores and retrieves the values that a VARIANT can hold.

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.

The following is an example of a global variable (boolWarnedOnPreviousLoop) that can be shared between scripts:

```
Storage.PersistValueExists("/boolWarnedOnPreviousLoop");
```

- "SetNameValue, NameValueExists, GetNameValue" on page 199
- "SetPersistString, PersistValueExists, GetPersistString" on page 199
- "RuleState" on page 199
- "RetrySeconds" on page 200

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)
```

D.5 Interfaces

These interfaces are returned by one of the methods of the namespaces described in Section D.4, “Script Namespaces,” on page 180 or by one of the methods or properties of the following interfaces:

- Section D.5.1, “IClientAdapter Interface,” on page 200
- Section D.5.2, “IClientEnvData Interface,” on page 202
- Section D.5.3, “IClientNetEnv Interface,” on page 203
- Section D.5.4, “IClientWAP Interface,” on page 209
- Section D.5.5, “IClientAdapterList Interface,” on page 209

D.5.1 IClientAdapter Interface

This interface returns information about an adapter.

- “GetNetworkEnvironment” on page 201
- “DeviceID” on page 202
- “Enabled” on page 202
- “IP” on page 202
- “MAC” on page 202
- “MaxSpeed” on page 202
- “Name” on page 202

- “SubNetMask” on page 202
- “Type” on page 202

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 “GetAdapters” on page 189.

Enabled

See “GetAdapters” on page 189.

IP

See “GetAdapters” on page 189.

MAC

See “GetAdapters” on page 189.

MaxSpeed

See “GetAdapters” on page 189.

Name

See “GetAdapters” on page 189.

SubNetMask

See “GetAdapters” on page 189.

Type

See “GetAdapters” on page 189.

D.5.2 IClientEnvData Interface

This interface returns environment data about a server or wireless access point.

- “IP” on page 202
- “MAC” on page 202
- “SSIP” on page 202
- “Type” on page 203

IP

See “GetLocationMatchData, LocationMatchCount” on page 190.

MAC

See “GetLocationMatchData, LocationMatchCount” on page 190.

SSIP

See “GetLocationMatchData, LocationMatchCount” on page 190.

Type

See “GetLocationMatchData, LocationMatchCount” on page 190.

D.5.3 IClientNetEnv Interface

This interface provides network environment information.

- “GetDHCPItem” on page 203
- “GetDNSItem” on page 204
- “GetGatewayItem” on page 205
- “GetWINSItem” on page 206
- “GetWirelessAPItem, WirelessAPCount” on page 207
- “DHCPCount” on page 208
- “DNSCount” on page 208
- “GatewayCount” on page 208
- “WINSCount” on page 209
- “WirelessAPCount” on page 209

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 “GetNetworkEnvironment” on page 201.

DNSCount

See “GetNetworkEnvironment” on page 201.

GatewayCount

See “GetNetworkEnvironment” on page 201.

WINSCount

See “GetNetworkEnvironment” on page 201.

WirelessAPCount

See “GetNetworkEnvironment” on page 201.

D.5.4 IClientWAP Interface

This interface provides information about a wireless access point.

- “AvgRssi” on page 209
- “MAC” on page 209
- “MaxRssi” on page 209
- “MinRssi” on page 209
- “Rssi” on page 209
- “SSID” on page 209

AvgRssi

See “GetWirelessAPItem, WirelessAPCount” on page 207.

MAC

See “GetWirelessAPItem, WirelessAPCount” on page 207.

MaxRssi

See “GetWirelessAPItem, WirelessAPCount” on page 207.

MinRssi

See “GetWirelessAPItem, WirelessAPCount” on page 207.

Rssi

See “GetWirelessAPItem, WirelessAPCount” on page 207.

SSID

See “GetWirelessAPItem, WirelessAPCount” on page 207.

D.5.5 IClientAdapterList Interface

This interface is a list of adapters in the network environment.

Item & Length

See “GetAdapters” on page 189.

D.6 Sample Scripts

The following sections contain sample scripts that you can use and modify:

- Section D.6.1, “Create Registry Shortcut (VBScript),” on page 210
- Section D.6.2, “Allow Only One Connection Type (JScript),” on page 212
- Section D.6.3, “Stamp Once Script,” on page 213

D.6.1 Create Registry Shortcut (VBScript)

This script is to run at startup of the 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 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. Modems are also disabled because 3G wireless cards 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
```

D.6.2 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);
}
```

D.6.3 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 Security Client does not permit additional network environments to be saved at that location.

NOTE: This script works best when it is used for an environment that probably won’t change its network parameters (for example, an user’s home network or a satellite office). If network identifiers change (such as IP or MAC addresses), the 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* for a policy in the Management Console, 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.

Shared Component Usage

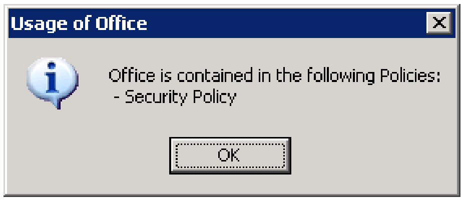
E

Many policy components (locations, network environments, firewalls, and so forth) can be shared among security policies.

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

1 Right-click the shared component and select *Show Usage*.

   A Usage dialog box lists each policy that is using the component.



Office is contained in the following Policies:
- Security Policy