User Guide

NetIQ® VigilEnt™ Policy Center

August 2011

Legal Notice

Contents

Chapter 3
Performing Post-Installation Tasks 21

Chapter 4
Setting the User Repository 35

Chapter 5
Controlling User Access 55

Chapter 6
Preparing for Document Management 71

Chapter 7
Developing Policy Documents 79

Chapter 8
Managing Policy Documents 97

Chapter 9
Creating and Managing Quizzes 109

Chapter 12
Managing Reporting 137

Chapter 13
Administering VPC 141

About This Book and the Library

The *User Guide* provides conceptual information about the NetIQ VigilEnt Policy Center (VPC) product. This book defines terminology and various related concepts. This book also provides an overview of the user interfaces and step-by-step guidance for many tasks.

Intended Audience

This book provides information for individuals responsible for understanding VPC concepts and for individuals designing and implementing a security solution for their enterprise network.

Other Information in the Library

The library provides the following information resources:

User Guide

Provides conceptual information and step-by-step guidance for common Administration Site tasks.

Help — Administration Site

Provides conceptual information and step-by-step guidance for common Administration Site tasks.

Help — User Site

Provides step-by-step guidance for common User Site tasks.

Tutorials

Provide interactive training for common VPC tasks performed in the Administration Site.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*value*]	• Optional parameters of a command
Braces, such as {*value*}	• Required parameters of a command
Logical OR, such as *value1 | value2*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

Chapter 1

Understanding VPC

Effective security policies are the cornerstone of any security effort. This effort includes writing policies, as well as communicating them to everyone who has access to and uses company information. Once you communicate the policies, you should measure how well the policies are communicated and understood by each employee. VigilEnt Policy Center (VPC) helps automate this entire process of security policy management.

Policy Challenges and the VPC Solution

Keeping policies up to date and making sure employees are aware of these changes is a complex but necessary procedure. As businesses grow and expand to include new companies, products, and regions, each with their own set of policies and standards, information security officers often ask themselves serious questions.

How do I avoid employees being careless with confidential information and costing us millions in revenue?

VigilEnt Policy Center helps educate employees about current policies and tests their knowledge through customized policy quizzes.

How can I prevent lawsuits stemming from new government legislation requirements in all our regions?

You can easily update any existing policy document or create new policies as technology and regulations change throughout your company's life.

How can I make users aware of email viruses that produce costly downtimes?

Using a company's intranet, you can instantly send news items and alert users of sudden events.

How do I get all this vital information to our offices and track whether anyone reads and understands it?

VPC lets you easily distribute policies around the world and verify that your users have received, read, and understood the current documents.

VigilEnt Policy Center is the first product to address these issues with a comprehensive security management solution.

VPC Architecture Overview

VigilEnt Policy Center has the following main components:

VigilEnt Policy Center Server

A Windows service that runs on the computer where VPC resides and provides access to the Administration Site and User Site.

Administration Site

An intranet Web site used for defining, publishing, and tracking policy documents and quizzes, setting company and user information, and following security incidents.

User Site

An intranet Web site used by employees to read policy documents, complete quizzes, view news items, and report security incidents.

The following figure shows how these components interact.

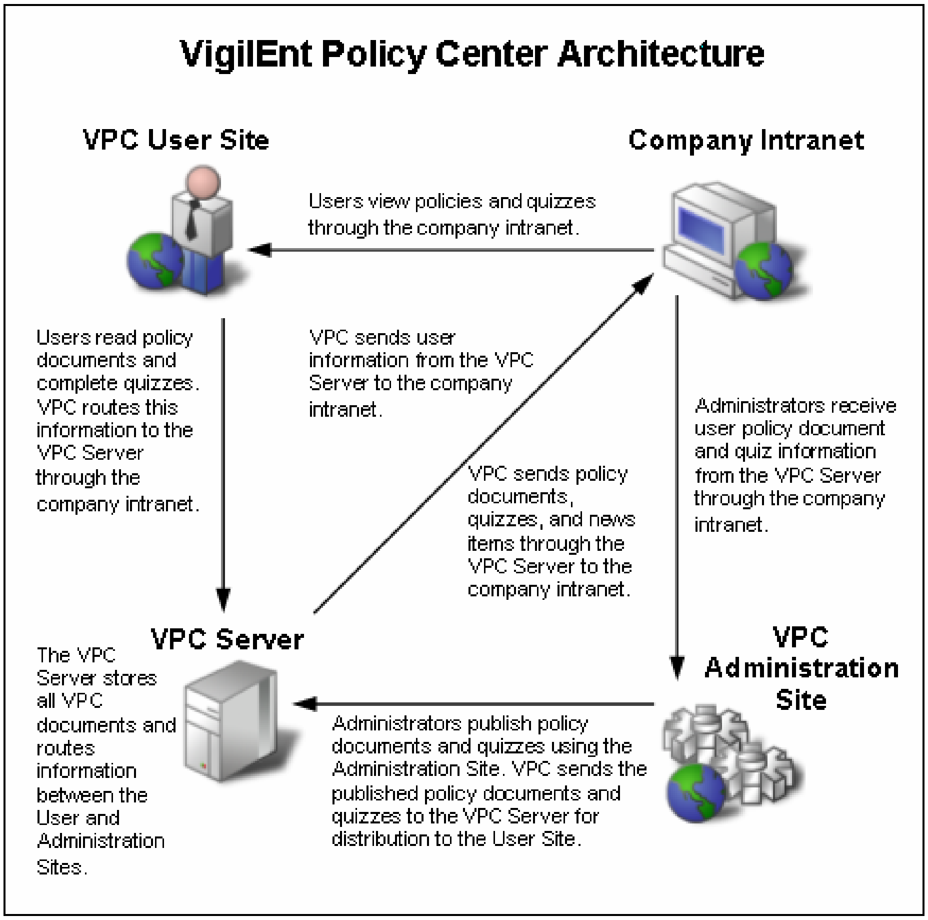

VigilEnt Policy Center Architecture
VPC User Site
Company Intranet
Users view policies and quizzes through the company intranet.
Users read policy documents and complete quizzes. VPC routes this information to the VPC Server through the company intranet.
VPC sends user information from the VPC Server to the company intranet.
VPC sends policy documents, quizzes, and news items through the VPC Server to the company intranet.
Administrators receive user policy document and quiz information from the VPC Server through the company intranet.
VPC Server
The VPC Server stores all VPC documents and routes information between the User and Administration Sites.
VPC Administration Site
Administrators publish policy documents and quizzes using the Administration Site. VPC sends the published policy documents and quizzes to the VPC Server for distribution to the User Site.

Figure 1. VPC Architecture

VigilEnt Policy Center Server

The VPC Server is a Windows service that runs on the computer where VigilEnt Policy Center resides, provides access to the Administration Site and User Site, and runs at all times. If the computer loses power, the service automatically starts when you restart the computer.

The VPC Server service displays as **VigilEnt Policy Center** in the Windows Services dialog box. Access this dialog box in the Windows operating system by opening **Services** in **Administrative Tools**.

Administration Site

The Administration Site is a central location where an information security officer can create and manage the policy documents, quizzes, and options used to educate users and control information security. The Administration Site helps companies adhere to government regulations that mandate strict policies and procedures for access to, and distribution of, confidential materials.

The Administration Site includes the following tabs to organize the various tasks required to manage documents, run reports, and administer VPC:

Home Tab

The Home tab provides a snapshot of the current state of VigilEnt Policy Center. The content ties directly to the default VPC roles and each user may see a different view. For example, a user logged on as a Power User sees different information than a user logged on as a VPC Administrator.

The Home tab can include a summary of policy status as well as links to recent documents and common administration tasks. VPC Administrators also see current license usage and VPC configuration information.

Policy Center Tab

The Policy Center tab includes the management of policy documents created in VigilEnt Policy Center or imported from another source. VPC groups policy statements by category and subcategory. Companies can import existing policy documents, create new documents, or decrease the time needed for policy document creation by using one of the provided policy document samples or templates when creating a new document.

Education Tab

The Education tab provides a measure of user comprehension of documents created in VigilEnt Policy Center. Administrators can create and publish quizzes to the User Site to test and grade users for comprehension. You can use quizzes as surveys to determine a particular unit’s level of comprehension, or as a risk assessment to evaluate the overall level of information security for a particular unit.

Reporting Tab

The Reporting tab provides several different reports for analyzing who has read and how well they understand policy documents by completing quizzes on specific policies. VigilEnt Policy Center includes User Reports, Policy Reports, and Quiz Reports. An administrator also can create and manage security incident reports using the Reporting tab.

Administration Tab

The Administration tab represents the key to the Administration Site and provides access to program configurations. Administrators can use this tab to create users and groups, grant permissions to users, set up access to policy documents and quizzes, manage the operations of the User Site, run administrative reports, and maintain security incident reporting.

User Site

The VPC User Site is a central location to distribute information security policies, procedures, quizzes, general news items, and receive feedback from users. VPC disseminates this information throughout the organization to each employee based on user ID. VPC offers reports to review the effectiveness and understanding of organization policies and procedures based on the information available in the User Site.

Users log on to the User Site through their access to a Web browser. From this site, users can read policy documents, complete quizzes, and view news items posted by an administrator. If an administrator sets certain permissions, users can review documents, create their own account, modify the account information, change their password, report a security incident, and change the language in which VPC displays the User Site.

Administrators set permissions for the User Site through the Administration Site and offer their users different options. For example, users can create their own accounts, edit their personal information, and report an incident, but only when the administrator sets the options in **Administration > User Site > Privileges**.

User Site Home Page

By default, VigilEnt Policy Center displays the Home page after a user logs on to the User Site. The Home page shows all new policy documents and quizzes that the logged on user has permission to view. Documents in Review state show with an “R” on the document icon. After reading a policy document, a user acknowledges that they have read and understood the policy, and VPC sends verification to the Administration Site. Users can also complete a quiz and view the score in the User Site. Like policy confirmations, VPC sends quiz scores to the Administration Site, so document managers can view and report results.

The User Site Home page also includes a **News** box, which displays informative items from the administrator. News items typically convey security news and information about a new policy document or quiz. The flexibility of the news item feature allows administrators to include text, graphics, and video files as news items.

About VPC Documents

Organizations typically use VPC to manage the following types of documents:

Policies

Security policy documents are important for audits and legal dispute resolution. Correctly written and implemented, policy documents act as a clear statement of management intentions, reducing potential liability.

Quizzes

Companies use quizzes to measure employee knowledge of current policy. A good practice consists of including a quiz for each policy document residing in VPC. You can set up a quiz with a minimum passing grade requirement, ensuring that users carefully read the policy document before completing the quiz. VPC offers the results in report form for use in an audit or as proof during a lawsuit.

You can convey information other than information security policies by using VPC. For example, a company may include a policy document and quiz on the proper protocol when flying a country’s flag while another uses VPC to inform users of the facts about a charitable organization benefiting from a company-sponsored event.

Assessments and Surveys

You can create assessments using the same functionality driving the quiz feature. Resembling a quiz, an assessment is a query used by an organization to evaluate regulatory requirement compliance or readiness for a specific situation. For example, the Cyberterrorism Readiness Self Assessment contains questions that focus on an organization's preparedness to protect itself from the threat of cyberterrorism. Unlike a quiz, VPC measures an assessment using a compliance percentage.

About VPC Libraries

VPC includes both a policy document library and quiz library to help you create effective documents for your organization.

Policy Document Library

The Policy Document Library contains collections of policy statements organized by industry standard or regulation. These include:

- **Basel II**: International Convergence of Capital Measurement and Capital Measurement
- **ISO 17799**: Code of Practice for Information Technology Management
- **NIST 800-53**: National Institute of Standards and Technology recommended security controls for federal information systems
- **PCI**: Payment Card Industry Data Security Standard
- **Sarbanes-Oxley**: H.R. 3763 Sarbanes-Oxley Act of 2002

You can use these comprehensive policy statement resources to assist in creating a complete set of policy documents and assessments to improve your organization's information security preparation, awareness, and resolution.

Quiz Library

The Quiz Library contains over 1,400 questions that you can use to create your quizzes and assessments. These questions are based on information security leading practices and policies, and you can use the questions in their current state or customize them for your specific needs. Each of these questions integrates with the VPC quiz editor, letting you create a new document with up-to-date security standards.

Chapter 2

Installing VigilEnt Policy Center

This chapter provides information about preparing for and installing VigilEnt Policy Center for the first time. For instructions on upgrading VPC from a previous version, see the *Release Notes*.

Understanding Deployment Options

Before installing and configuring VPC, it is important to determine the database source you want VPC to use for users and group data. It is also important to select the authentication mechanism for VPC to use when users log onto VPC.

User Repository Deployment Options

You can store a set of users and groups in the VPC database or configure VPC to use the users and groups stored in one or more LDAP-compliant databases.

When you use VPC as the user repository, you import user and group information from an outside source. This practice duplicates your user and group information and requires maintaining the data in two places. Furthermore, user IDs and passwords on the network are not synchronized with those in VPC, so users enter a user ID and password to log onto VPC unless the credentials are exactly the same.

Most large organizations use an external user repository for increased speed, additional security, and reduced administration costs. Rather than importing the user data into VPC, you access user and group data from any LDAP-compliant server, such as Windows 2000 or later Active Directory or Microsoft Exchange.

You can also point VPC to use multiple repositories including using both the internal and external repositories at the same time. Organizations that have complex LDAP-enabled repositories can navigate all users and groups through VPC no matter the repository in which each user or group resides. To avoid confusion when duplicate user ID and group names exist, VPC displays the data in the following format: *userorgroupname@repositoryname*.

User Authentication Deployment Options

VPC offers two methods to authenticate users when they log onto VPC. You can use the Tomcat Web server that installs with VPC, or you can configure VPC to run with another Web server, such as Microsoft Internet Information Server (IIS). The VPC Web server provides standard security options and authentication speed; however, with this configuration users provide a user name and password when they log onto VPC. The following figure shows how each component works together for logging on to VPC when you use VPC to authenticate users.

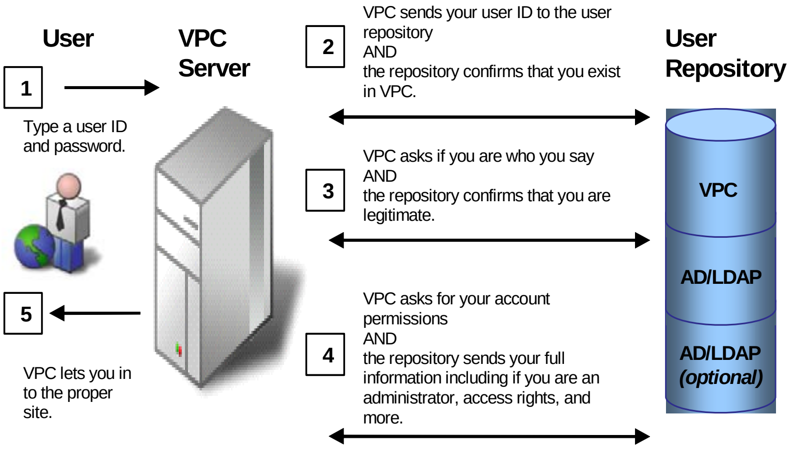

User
VPC Server
User Repository
1
Type a user ID and password.
2
VPC sends your user ID to the user repository AND the repository confirms that you exist in VPC.
3
VPC asks if you are who you say AND the repository confirms that you are legitimate.
4
VPC asks for your account permissions AND the repository sends your full information including if you are an administrator, access rights, and more.
5
VPC lets you in to the proper site.
VPC
AD/LDAP
AD/LDAP (optional)

Figure 2. VPC user authentication process

Alternately, you can configure VPC to run with another Web server, such as a Microsoft Internet Information Server (IIS). With this configuration, users do not have to provide a user name and password when they log onto VPC because the Web server automatically authenticates with the credentials stored in the designated user repository. For more information, see "Configuring IIS Authentication" on page 49. Using an external Web server also increases authentication response speed and provides additional security options, such as extra NTFS security and digital certificates. The following figure shows how each component works together for logging on to VPC using an external Web server for authentication.

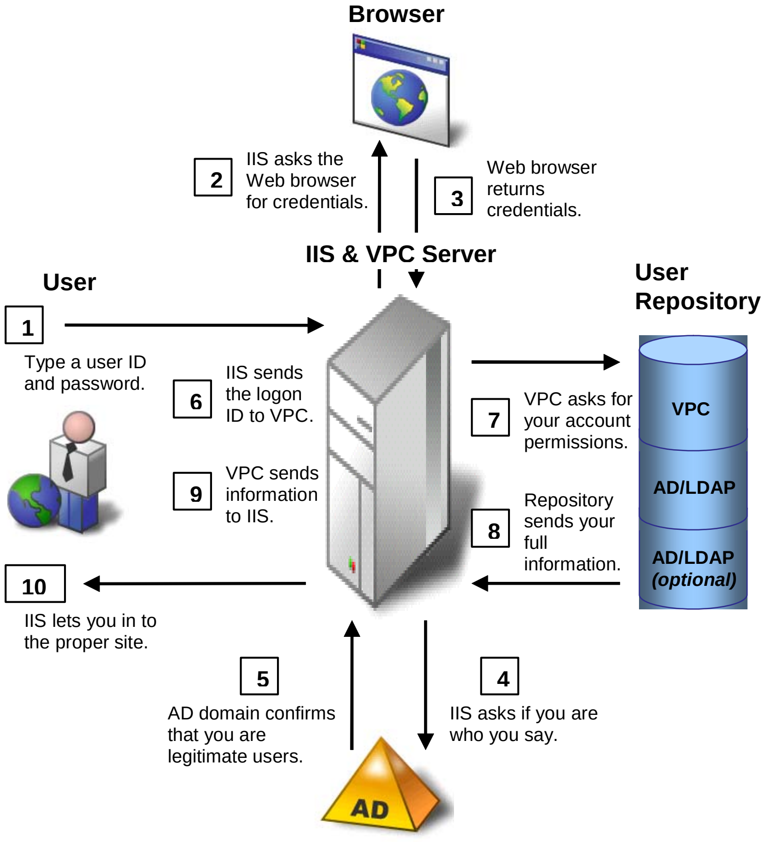

Browser
2
IIS asks the Web browser for credentials.
3
Web browser returns credentials.
IIS & VPC Server
User
User Repository
1
Type a user ID and password.
6
IIS sends the logon ID to VPC.
9
VPC sends information to IIS.
7
VPC asks for your account permissions.
8
Repository sends your full information.
VPC
AD/LDAP
AD/LDAP (optional)
10
IIS lets you in to the proper site.
5
AD domain confirms that you are legitimate users.
4
IIS asks if you are who you say.
AD

Figure 3. VPC authentication process using an external Web server

Determining Installation Requirements

Hardware and software requirements for the computer hosting the VPC components vary by the number of users in the environment. This section describes how to determine the requirements necessary for your installation of VPC.

Requirements for Fewer Than 1,000 Users

The following table describes the recommended hardware and software requirements for the VPC server computer in environments with fewer than 1,000 users. The VPC server computer should have direct connection to the company intranet.

Component	Requirement
CPU	Intel Pentium 866 MHz
RAM	256 MB minimum, 512 MB recommended
Operating System	Microsoft Windows 2000 Server, or Windows Server 2003, 2008, or 2008 R2, with available service packs.
Database	Microsoft SQL Server 2000, 2005, 2005 Express, or 2008, with available service packs (recommended). ***If you are using Microsoft SQL Server 2005 or 2008,*** do not use the dynamic port assignment configuration option. VPC uses port 1433, unless you assign a different port during installation, and does not function correctly if SQL Server is configured to dynamically assign a port. VPC does not require a dedicated Microsoft SQL Server installation. VPC can co-exist with other database applications or use SQL Server with multiple instances. Because VPC has multiple connections to SQL Server, verify that you have enough licenses to cover the projected number of concurrent users.
Web Component (optional)	For pass-through authentication, Microsoft Internet Information Server (IIS) 6.0 or 7.0.
Web Browser	One of the following Web browsers: • Internet Explorer 6.0 through 8.0 • Netscape 7.0 • Firefox 1.0 through 3.5 Note: To view and use most VPC features, you can use a supported version of Netscape or Firefox. However, to edit Microsoft Word documents using ActiveX controls, you must access VPC through Internet Explorer. Although Firefox and other browsers that work on multiple operating systems use the Netscape Plugin Application Programming Interface (NPAPI) system, which performs functions similar to those of ActiveX, Firefox does not officially support ActiveX.

Requirements for 1,000 to 5,000 Users

The following table describes the recommended hardware and software requirements for the VPC server computer in environments with 1,000 to 5,000 users. The VPC server computer should have direct connection to the company intranet.

Component	Requirement
CPU	Intel Pentium 1 GHz with 256 MB cache
RAM	1 GB SDRAM
Hard Drive	Two (2) 18 GB RAID-configured SCSI hard drives The VPC Server stores imported documents in DOC, DOCX, and PDF file format. Therefore, also allow for the size and number of documents you plan to import into VPC.
Network Interface Card	100 MB or 1 GB, depending upon its placement on the network
Operating System	Microsoft Windows 2000 Server, or Windows Server 2003, 2008, or 2008 R2, with available service packs.

Component	Requirement
Database	Microsoft SQL Server 2000, 2005, 2005 Express, or 2008, with available service packs (recommended). ***If you are using Microsoft SQL Server 2005 or 2008,*** do not use the dynamic port assignment configuration option. VPC uses port 1433, unless you assign a different port during installation, and does not function correctly if SQL Server is configured to dynamically assign a port. VPC does not require a dedicated Microsoft SQL Server installation. VPC can co-exist with other database applications or use SQL Server with multiple instances. Because VPC has multiple connections to SQL Server, verify that you have enough licenses to cover the projected number of concurrent users.
Web Component (optional)	For pass-through authentication, Microsoft Internet Information Server (IIS) 6.0 or 7.0.
Web Browser	One of the following Web browsers: • Internet Explorer 6.0 through 8.0 • Netscape 7.0 • Firefox 1.0 through 3.5 Note: To view and use most VPC features, you can use a supported version of Netscape or Firefox. However, to edit Microsoft Word documents using ActiveX controls, you must access VPC through Internet Explorer. Although Firefox and other browsers that work on multiple operating systems use the Netscape Plugin Application Programming Interface (NPAPI) system, which performs functions similar to those of ActiveX, Firefox does not officially support ActiveX.

Requirements for 5,000 to 10,000 Users

The following table describes the recommended hardware and software requirements for the VPC server computer in environments with 5,000 to 10,000 users. The VPC server computer should have direct connection to the company intranet.

Component	Requirement
CPU	Dual Pentium 2 GHz with 256 MB cache
RAM	4 GB SDRAM or higher
Hard Drive	Two (2) 18 GB RAID-configured SCSI hard drives The VPC Server stores imported documents in DOC, DOCX, and PDF file format. Therefore, also allow for the size and number of documents you plan to import into VPC.
Network Interface Card	100 MB or 1 GB, depending upon its placement on the network
Operating System	Microsoft Windows 2000 Server, or Windows Server 2003, 2008, or 2008 R2, with available service packs.
Database	Microsoft SQL Server 2000, 2005, 2005 Express, or 2008, with available service packs (recommended). ***If you are using Microsoft SQL Server 2005 or 2008,*** do not use the dynamic port assignment configuration option. VPC uses port 1433, unless you assign a different port during installation, and does not function correctly if SQL Server is configured to dynamically assign a port. VPC does not require a dedicated Microsoft SQL Server installation. VPC can co-exist with other database applications or use SQL Server with multiple instances. Because VPC has multiple connections to SQL Server, verify that you have enough licenses to cover the projected number of concurrent users.

Component	Requirement
Web Component (optional)	For pass-through authentication, Microsoft Internet Information Server (IIS) 6.0 or 7.0.
Web Browser	One of the following Web browsers: • Internet Explorer 6.0 through 8.0 • Netscape 7.0 • Firefox 1.0 through 3.5 Note: To view and use most VPC features, you can use a supported version of Netscape or Firefox. However, to edit Microsoft Word documents using ActiveX controls, you must access VPC through Internet Explorer. Although Firefox and other browsers that work on multiple operating systems use the Netscape Plugin Application Programming Interface (NPAPI) system, which performs functions similar to those of ActiveX, Firefox does not officially support ActiveX.

Requirements for More Than 10,000 Users

If you have more than 10,000 users, NetIQ Corporation recommends using at least two servers: one for the VPC Server and one for the VPC Database. VPC does not require at least two servers, but additional servers improve performance of VPC in very large environments.

Computer One: VPC Server Computer

The following table describes the recommended hardware and software requirements for the VPC server computer in environments with more than 10,000 users. The VPC server computer should have membership in the company domain and direct connection to the company intranet.

Component	Requirement
CPU	Dual Pentium 3 GHz (ideal) with 256 MB cache processors minimum (quad processors, if possible)
RAM	4 GB SDRAM or higher
Hard Drive	Two (2) 18 GB RAID-configured SCSI hard drives with 100 GB free disk space The VPC Server stores imported documents in DOC, DOCX, and PDF file format. Therefore, also allow for the size and number of documents you plan to import into VPC.
Network Interface Card	100 MB or 1 GB, depending upon its placement on the network
Operating System	Microsoft Windows 2000 Server, or Windows Server 2003, 2008, or 2008 R2, with available service packs.
Web Component (optional)	For pass-through authentication, Microsoft Internet Information Server (IIS) 6.0 or 7.0.
Web Browser	One of the following Web browsers: • Internet Explorer 6.0 through 8.0 • Netscape 7.0 • Firefox 1.0 through 3.5 Note: To view and use most VPC features, you can use a supported version of Netscape or Firefox. However, to edit Microsoft Word documents using ActiveX controls, you must access VPC through Internet Explorer. Although Firefox and other browsers that work on multiple operating systems use the Netscape Plugin Application Programming Interface (NPAPI) system, which performs functions similar to those of ActiveX, Firefox does not officially support ActiveX.

Computer Two: Database Computer

The following table describes the recommended hardware and software requirements for the VPC database computer in environments with more than 10,000 users. The VPC database computer should have membership in the company domain.

Component	Requirement
CPU	Dual Pentium 3 GHz (ideal) with 256 MB cache processors minimum (quad processors, if possible)
RAM	4 GB SDRAM or higher
Hard Drive	Two (2) 18 GB RAID-configured SCSI hard drives with 100 GB free disk space. The VPC Server stores imported documents in DOC, DOCX, and PDF file format. Therefore, also allow for the size and number of documents you plan to import into VPC.
Network Interface Card	100 MB or 1 GB, depending upon its placement on the network
Operating System	Microsoft Windows 2000 Server, or Windows Server 2003, 2008, or 2008 R2, with available service packs.
Database	Microsoft SQL Server 2000, 2005, 2005 Express, or 2008, with available service packs (recommended). ***If you are using Microsoft SQL Server 2005 or 2008,*** do not use the dynamic port assignment configuration option. VPC uses port 1433, unless you assign a different port during installation, and does not function correctly if SQL Server is configured to dynamically assign a port. VPC does not require a dedicated Microsoft SQL Server installation. VPC can co-exist with other database applications or use SQL Server with multiple instances. Because VPC has multiple connections to SQL Server, verify that you have enough licenses to cover the projected number of concurrent users.
Web Component (optional)	For pass-through authentication, Microsoft Internet Information Server (IIS) 6.0 or 7.0.
Web Browser	One of the following Web browsers: • Internet Explorer 6.0 through 8.0 • Netscape 7.0 • Firefox 1.0 through 3.5

Note

Although VPC leverages the proxy account vpc_user to connect to the SQL Server database, VPC requires multiple connections to SQL Server. Therefore, verify that you have enough licenses to cover the projected number of concurrent users. NetIQ Corporation recommends **Per Processor** licensing for SQL Server. **Per Server and Device** and **Per User** licensing can become cost prohibitive in very large environments. The **Per Processor** licensing model requires a license for each physical or virtual processor accessed by an operating system environment running SQL Server. This license does not require any device or user client access licenses (CALs). SQL Server Enterprise Edition does not limit the number of connections and is ideal for organizations that expect high transaction volume to VPC.

User Computer Requirements

Access to the Administration Site or User Site requires users to have one of the following browsers:

- Internet Explorer 6.0 through 8.0
- Netscape 7.0
- Firefox 1.0 through 3.5

Note
To view and use most VPC features, you can use a supported version of Netscape or Firefox. However, to edit Microsoft Word documents using ActiveX controls, you must access VPC through Internet Explorer. Although Firefox and other browsers that work on multiple operating systems use the Netscape Plugin Application Programming Interface (NPAPI) system, which performs functions similar to those of ActiveX, Firefox does not officially support ActiveX.

Microsoft Word Document Requirements

To work with and manage Microsoft Word documents in VPC, user computers must meet the following requirements:

- Microsoft Word 2003 or 2007
- Monitor resolution set to 1024 by 768 pixels or more
- Internet Explorer 6.0, 7.0, or 8.0 with local intranet security settings enabled for ActiveX as shown in the following table.

Note
The settings shown in the table are the default settings when your security setting is **Medium** or **Medium-Low**. For detailed instructions on setting browser security for the VPC Word Editor, see "Setting Your Browser to Use the Word Editor" on page 90.

Setting	Permission
Download signed ActiveX controls	Prompt
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe for scripting	Disable
RunActiveX controls and plug-ins	Enable
Script ActiveX controls marked safe for scripting	Enable

Adobe PDF Document Requirements

To view PDF documents in VPC, user computers require Adobe Acrobat or Adobe Reader.

Installing VPC

The procedures in this section guide you through the process of preparing the environment for installation, gathering the necessary installation information, and installing the VPC components.

Gathering Installation Information

When installing VPC for the first time, provide the following information during the installation process. We recommend gathering this information before you begin the installation.

- A destination folder to store the VPC files. The default is `C:\Program Files\NetIQ\VigilEnt Policy Center`.
- The name of the Microsoft SQL Server to host the VPC database and the name of the SQL Server administrator ID and associated password. The default SQL Server name is `MSSQL` and the default administrator ID is `sa`.
- A Web server port number. The default is `8080`.
- An administrator ID and password. The default administrator ID is `admin`.
- A license key, which you receive at the time of purchase.

Setting MS SQL Server for TCP/IP Connections

Configure Microsoft SQL Server to use the TCP/IP networking protocol for VigilEnt Policy Center to access the SQL Server database. Use the following steps to set up MS SQL Server to accept the TCP/IP connections.

Note

VigilEnt Policy Center has multiple connections to your SQL Server database. Verify that you have enough SQL Server licenses to cover your projected number of concurrent users.

Be sure to perform this task before attempting the VPC installation.

To configure Microsoft SQL Server for TCP/IP connections:

1. Open **Microsoft SQL Server > Enterprise Manager**.
2. Select the server for connection, and from the **Action** menu select **Properties**.
3. Click **Network Configuration**.
4. Verify that the **Enabled protocols** list includes **TCP/IP**. If the list does not include **TCP/IP**, click **TCP/IP** from the **Disabled protocols** list, and then click **Enable**.
5. Click **TCP/IP** from the **Enabled protocols** list, and then click **Properties**.
6. ***If you are using Microsoft SQL Server 2000 or 2008***, verify that the default port number is `1433`.
7. ***If you are using Microsoft SQL Server 2005 Express***, verify that the default port number is `1435`. Type a different port number if the port number is in use.

   Note

   Although you can configure a server to any port number, the default for Microsoft SQL Server 2000 and 2008 is `1433` and the default for Microsoft SQL Server 2005 Express is `1435`. Any port number works, but if an administrator changes the number from the default, be sure to select a different port from the one used by VigilEnt Policy Center.

   If the number entered is already in use, VPC displays the Select New Port Number dialog box. The dialog box displays an unused port number for selection or you can type a different number in the field.

8. Close the Network Configuration window, and then close the SQL Server Properties window.

Enabling Microsoft SQL Server Authentication

VigilEnt Policy Center uses Microsoft SQL Server authentication to connect to the database. After setting Microsoft IIS support, most administrators want to configure VigilEnt Policy Center to authenticate users through the Web server. This feature lets users who are authenticated against the Windows domain directly connect to the User Site without having to log on again. Configure Microsoft SQL Server with mixed authentication mode so SQL Server and Windows authentication are enabled by default.

Note
Ensure you perform this task before attempting the VigilEnt Policy Center installation.

To enable Microsoft SQL Server authentication:

1. ***If you are using Microsoft SQL Server 2000***, complete the following steps:

   a. Open **Microsoft SQL Server > Enterprise Manager**.

   b. Select the server for connection, and from the **Action** menu select **Properties**.

   c. Click **Security**, and then select **SQL Server and Windows**.

   d. Click **OK**.

2. ***If you are using Microsoft SQL Server 2005, 2005 Express, or 2008***, complete the following steps:

   a. Open SQL Server Management Studio.

   b. Connect to the database server using the `sa` account provided during the installation.

   c. Right-click the server and select **Properties**.

   d. Click **Security**.

   e. Select **SQL Server and Windows Authentication mode** and click **OK**.

Installing the VPC Components

The following steps describe how to install VPC for the first time. For instructions on upgrading VPC from a previous version, see the *Release Notes*.

Install VigilEnt Policy Center using an account with administrator permissions for the computer on which you are attempting to run the VPC installation program. If the account does not have local administrator permissions, your computer displays an error message and closes the installation program.

To install VigilEnt Policy Center:

1. Log on to the computer using a local administrator account.

2. Select `Setup.exe` in the root folder of the VPC installation kit, and then from the **File** menu, click **Open**.

   VPC displays the autorun setup page.

3. Click **Begin Setup**.

   The installation program displays the Welcome dialog box. Be sure to exit all programs before continuing.

4. Click **Next**.

   The installation program displays the License Agreement dialog box. Be sure to read all of the information in this dialog box before proceeding.

5. Click **I Agree** to agree to the licensing terms, and then click **Next**.

   The installation program displays the Registration Information dialog box.

6. In the **Company** field, type the name of the organization that owns the license, and then click **Next**.

   The installation program displays the Choose Destination Location dialog box. The default location for the VPC files is `C:\Program Files\NetIQ\VigilEnt Policy Center`.

7. ***If you want to select a location other than the default installation folder***, click **Browse** and find the appropriate location. Otherwise, click **Next**.

   The installation program displays the Select Security Certificate dialog box.

8. ***If you want to secure your HTTP communication by using secure sockets***, click **Yes, use secure sockets**, and continue with the next step. ***If you do not want to use secure sockets***, click **No, do not use secure sockets**, and continue with Step 10.

9. In the **Certificate File** field, type the path for the file containing certificate information or click **Browse** to search. VigilEnt Policy Center includes a sample certificate. You can accept the default or select your own certificate.

10. Click **Next**.

    The installation program displays the Set Web Server Port Number dialog box.

11. Verify that the **Port Number** field shows the default `8080` if you are not using SSL, `8443` if you are using SSL. If the network is using this port, type a different number, and then click **Next**.

    Note
    If the network is using this port, VPC displays the Select New Port Number dialog box including an unused port number for selection. You also can type a different number in the field.

    The installation program displays the Set Default Administrator ID and Password dialog box.

12. Type the administrator account ID in the **Administrator ID** field.

    Note
    You cannot change the **Administrator ID** after installing VigilEnt Policy Center.

13. Type a password in the **Password** field and confirm by typing the same password in the **Verify Password** field.

14. Click **Next**.

    The installation program displays the Enter License Key dialog box. You receive a license key upon purchasing VPC. If you do not have a license key, contact NetIQ Technical Support.

15. Type the alphanumeric key in the **License Key** field, and then click **Next**.

    The installation program displays the Select Content to Install dialog box.

16. Click **Install Sample Content** if you want document samples in your version of VPC, and then click **Next**.

    The installation program displays the Enter Database Name dialog box.

17. In the **Application Database Name** field, type the name that you want VPC to use as a database, and then click **Next**.

    The installation program displays the Enter SQL Server TCP/IP Connection Data dialog box. Use this dialog box to enter the SQL Server connection information.

18. In the **MS SQL Server Host Name or IP Address** field, type the name of the computer hosting SQL Server.

19. Type the TCP/IP port number in the **MS SQL Server TCP/IP Port Number** field.

    Note

    You may need to configure SQL Server for TCP/IP connections. For more information, see “Setting MS SQL Server for TCP/IP Connections.”

20. Click **Next**.

    The installation program displays the Enter SQL Server Administration Data dialog box. Use this dialog box to enter the SQL Server administration information.

    Note

    Enable the database creator and security administrator roles before adding the Microsoft SQL Server administrator account to the VPC installation program.

21. Type the SQL Server administrator ID in the **MS SQL Server Administrator ID** field and the password in the **MS SQL Server Administrator Password** field, and then click **Next**.

    The installation program displays the Enter VPC Database Account Data dialog box.

22. Type the user ID for the SQL Server user account in the **Database User ID** field. This account is the logon account in MS SQL Server through which VPC accesses the database.

23. Type a password in the **Database User Password** field and confirm by typing the same password in the **Check Password** field.

    Note

    NetIQ recommends that you enter a secure password that complies with your organization's security policies. Do not leave the password field blank. For more information about password security recommendations, contact Technical Support.

24. Click **Next**.

    VigilEnt Policy Center begins the installation.

    Note

    VPC may display error dialog boxes during this part of installation. If errors occur, read the dialog box carefully and follow the directions to clear the error. For example, VPC displays the Select New Port Number dialog box if the selected port number is in use. Click the suggested port number or type a new entry before continuing.

    The installation program displays the Installation Complete dialog box.

25. Click **Show Release Notes File** to view the Release Notes, and then click **Finish**.

Verifying the Installation

After completing the installation wizard, verify the installation was successful by logging onto the Administration Site and User Site. You may also want to view the files that the installation wizard installed.

Understanding the Folder Structure

VigilEnt Policy Center files install by default into `C:\Program Files\NetIQ\VigilEnt Policy Center`. The following table shows the contents of each major folder placed during installation.

<VPC Root Folder>	File Contents
`...\BACKUP`	Backup copies of files replaced during installation.
`...\bin`	Utility scripts, program executables, and files used for supporting Microsoft Internet Information Server (IIS).
`...\database`	Database files used by the VPC embedded database. For organizations that are using Microsoft SQL Server, the "policy" subfolder contains the XML files used to initialize the sample documents and libraries for VPC.
`...\Documentation`	*User Guide*, *Web Services Guide*, *Quick Preview, Release Notes*, and third-party software acknowledgement document.
`...\Examples`	Sample user list to import during evaluation and example VPC policy in French.
`...\server`	VPC Server configuration files, the Java Runtime Environment used to execute the VPC Server, library files, VPC logging information, static HTML files and Web server libraries, and the temporary files and directories that VPC uses during operation.

Logging onto the Administration and User Sites

Use the following procedures to log on to and off from each console.

Note

If you installed VPC on a Windows 2008 computer and Windows Firewall is turned on, Internet Explorer may display an error when you try to access either the Administration Site or the User Site. Turning off the firewall is not recommended, but you can open a port through the firewall to allow access to VPC. In Control Panel, open **Windows Firewall** and select the option to allow a program through the firewall. Add the port you specified when you installed VPC (the default is 8080). For more information about Windows Firewall, see the Windows 2008 documentation.

To log on to the Administration Site:

1. Select the **Administration Site** from the location where VPC resides. ***If you used the default settings during installation***, from the **Start** menu, select **... > NetIQ > VigilEnt Policy Center > Administration Site**.
2. Type the administrator ID in the **User ID** field and the password in the **Password** field, and then click **Log On**.

   Note

   If you set up multiple repositories, VPC changes the logon process and allows you to select a specific repository when you log on to the computer.

To log off from the Administration Site:

To log off from VPC, click **Log Off** in the upper right-hand corner of VPC.

To log on to the User Site:

1. Select the **User Site** from the location where the site resides. ***If you used the default settings during installation***, from the **Start** menu, select **... > NetIQ > VigilEnt Policy Center > User Site**.
2. *Optional.* Select the language in which you want to view your User Site.

3. Type the user ID in the **User ID** field and the password in the **Password** field, and then click **Log On**. VPC displays the Home page.

Note
If you set up multiple repositories, VPC changes the log-on process and allows you to select a specific repository when you log on to the computer.

To log off from the User Site:

To log off from VPC, click **Log Off** on the Home page.

Understanding Licensing

When you install VPC for the first time, VPC automatically validates your license for the number of users and expiration date during installation. VPC is licensed per active user and each user counts toward the license limit. VPC considers a user active if the user has read a policy document or completed a quiz within six months from the current date. If a user has not read a policy document or completed a quiz in the past year, VPC considers the user inactive and releases that user space within the license. VigilEnt Policy Center prompts the administrator with a warning when the VPC license count is within 25% of the total licenses available.

You can view your license information on the Home tab of the Administration Site when you are logged on as an administrator. You can also view licensing information by clicking **About** on the Administration tab.

Note
For additional information about licensing and distribution, contact Technical Support.

Chapter 3
Performing Post-Installation Tasks

After installing the VigilEnt Policy Center components, you may want to perform some additional configuration tasks. This chapter provides information about post-configuration tasks and how to perform them.

Enabling SSL Using Digital Certificates

If you enabled SSL during installation, replace the demo server certificate that installs with VPC because the certificate does not fully secure the browser-to-console communication. Replace the demo server certificate with a server certificate from a well-known and trusted Certificate Authority (CA) such as VeriSign.

To ensure the replacement of the demo server certificate, when you enable SSL, the computer displays a warning each time you access the Administration Site or User Site until you replace the demo server certificate.

Understanding Browser-to-Server Communication

When you make a connection to a secure Web server, the server authenticates itself. This authentication is a complex process involving public and private keys, and a digital certificate. A digital certificate is a verification from an independent third party that the server belongs to the company to which the server claims to belong. The certificate also provides the confidence that the server sends sensitive personal information to the right place.

A certificate authority (CA) issues these certificates. A CA is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate.

About Digital Certificates

A digital certificate is a binary file that contains the owner's name and identifying information along with a public key. A public key tells correspondents that the key belongs to a specific individual. Digital certificates generally contain a serial number, expiration date, and information about the rights, uses, and permissions associated with the certificate. In addition, the digital certificate contains information about the certificate authority who issued the certificate. All certificates are digitally signed using the private key of the certificate authority. Generally, software packages widely deploy the CA's own certificate, called a root certificate, letting people seamlessly identify legitimate certificates issued by the certification authority. If the CA maintains good security protection of the private key, it is virtually impossible for anyone to forge a digital certificate.

Using a Certificate with Microsoft Internet Explorer

When you type a URL in Microsoft Internet Explorer, the browser displays the security warning, "You are about to view pages over a secure connection. Any information you exchange with this Web site cannot be viewed by anyone else on the Web." Click **OK** to continue. If the security certificate on the site is issued by an untrusted company, the browser displays the security warning, "Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate." View the certificate before determining whether to trust the certifying authority.

Using a Certificate with Netscape Navigator

When you type a URL in Netscape Navigator, the browser displays the security warning, "You have requested a secure document. The document and any information you send back are encrypted for privacy while in transit." Click **OK** to continue. The computer displays a security wizard. Select one of the following choices from the wizard:

Accept this certificate permanently

The security message does not display on subsequent visits to the site.

Accept this certificate temporarily for this session

The security message does not display again until you close and then re-open the browser.

Do not accept this certificate and do not connect to the web site

Prevents the Web site access.

Replacing the Demo Server Certificate

Perform the following steps to replace the demo server certificate with a server certificate issued by a certificate authority (CA). First, create a server certificate key pair. Second, because companies are more likely to trust a certificate signed by a CA, create a certificate signing request (CSR). Finally, import a certificate for the CA.

Note

The shortcut from the Start menu no longer works after adding or deleting a digital certificate. Create a new shortcut because replacing the demo server certificate changes the URL.

To create a server certificate key pair:

1. Open Windows Explorer.
2. ***If you used the VPC default installation path***, select **... > NetIQ > VigilEnt Policy Center > server > conf**. ***If you customized your VPC installation***, find and open the conf folder.
3. Click **keystore.dat**, and then click the **Delete** icon.

   The computer displays a verification message.
4. Click **Yes**.
5. At a command or shell prompt, change to the `install_folder/bin` folder.
6. Type the following data:

   ```
   sslkey create
   ```

The computer prompts for the server name of first name, last name, organizational unit, such as “IT,” “Sales,” or “R&D”, organization name, such as your company name, city, state, and two-letter country code.

7. Enter the appropriate information *all in lowercase* after each prompt.

Note
When prompted for a first and last name, type the fully-qualified name of the Web site that you want to secure. If you run the Console on the host where you installed the Admin Agent and Local Agent, use `localhost` as the fully-qualified name.

Do not use commas in any of the prompts. Some of the trusted Certificate Authorities have problems with values that contain commas.

8. Accept the confirmation message that a 1024-bit RSA key pair and self-signed certificate (MD5 with RSA) were generated.

To create a certificate signing request:

1. At a command or shell prompt, change to the `install_folder/bin` folder.
2. Type the following data:

   ```
   sslkey request > request.txt
   ```

   The system writes the CSR to the `request.txt` file.
3. Submit this file to a CA, which authenticates the request and returns a certificate signed by the CA that authenticates the public key.

To import a certificate from the certificate authority:

1. At a command or shell prompt, change to the `install_folder/bin` folder.
2. Type the following data, where *certificate.cer* represents the name of the file that contains the certificate from the CA:

   ```
   sslkey import > certificate.cer
   ```

Suppressing the Digital Certificate

If you want to prevent your server from accessing the digital certificate, use the following steps.

Note
The shortcut from the Start menu no longer works after adding or deleting a digital certificate. Create a new shortcut because replacing the demo server certificate changes the URL.

To suppress a digital certificate:

1. Select **Administrative Tools > Services**.

   The computer displays the Services window.
2. Select **VigilEnt Policy Center**, and then from the **Action** menu click **Stop**.
3. Open the `server.xml` file in a DOS environment.
4. Delete the following lines:

   ```
   <!-- to disable HTTPS, remove the following parameters -->
   <Parameter name=“socketFactory” value=
   ```

```
“org.apache.tomcat.net.SSLSocketFactory”/>
<Parameter name= “keystore” value= “ ... /conf/keystore.dat”/>
<Parameter name= “keypass” value= “policy”/>
```

5. Save the file.

6. Restart the VigilEnt Policy Center service by accessing the Services window, selecting **VigilEnt Policy Center**, and then from the Action menu clicking **Start**.

Setting Audit Logging

You can set VPC to log the complete history of policies, quizzes, incidents, news items, users, and various actions taken in VPC. It is important that you enable audit logging before activating some properties within VPC. VPC displays a note about activating the related logging options when you attempt to activate certain properties.

Understanding Logging Options

When you set up audit logging, you specify which actions you want VPC to log, and for each action, where you want to log the information. You can log information to the VPC database, the Windows Event Log, or a separate VPC log file.

Logging Locations

For each action, VPC can log to the locations listed in the following table.

Logging Location	Abbreviation	Retrieval Method
VPC database	DB	Run audit reports from the Administration Site (see “Running an Audit Report”)
Windows Event Log	EL	View in the Windows Event Viewer
VPC log file	File	View the log file specified in Step 6 of this procedure (see “Viewing an Audit Log”)

Logging Options

The following tables describe the actions available for logging.

Application — Access Option	Purpose
Administration Site log on	Tracks the date and time that a user logged on to the Administration Site.
Administration Site log off	Tracks the date and time that a user logged off from the Administration Site.
Administration Site log on failure	Tracks the date and time that a user attempted to log on to the Administration Site, but the logon attempt failed.
User Site log on	Tracks the date and time that a user logged on to the User Site.

Application — Access Option	Purpose
User Site log off	Tracks the date and time that a user logged off from the User Site.
User Site log on failure	Tracks the date and time that a user attempted to log on to the User Site, but the logon attempt failed.

Application — Administrative Option	Purpose
Changes to audit logging options	Tracks the date and time that an administrator changed the option being logged within VPC. You cannot disable this option.
Diagnostics logging enabled	Tracks the date and time that an administrator enabled diagnostics.
Diagnostics logging disabled	Tracks the date and time that an administrator disabled diagnostics.
Purging of compliance data	Tracks the date and time that an administrator purged compliance data.
License key changed	Tracks the date and time that an administrator updated the license key.
Mail options changed	Tracks the date and time that an administrator modified the mail options.
Admin password changed	Tracks the date and time that an administrator changed the VPC Administrator account password.
Database connection password changed	Tracks the date and time that an administrator changed the database connection password.
Custom property added	Tracks the date and time that an administrator added a document custom property.
Custom property deleted	Tracks the date and time that an administrator deleted a document custom property.
User comments enabled	Tracks the date and time that an administrator enabled the ability for users to add comments on the User Site.
User comments disabled	Tracks the date and time that an administrator disabled the ability for users to add comments on the User Site.
Reviewer comments enabled	Tracks the date and time that an administrator enabled the ability for reviewers to add comments on the User Site.
Reviewer comments disabled	Tracks the date and time that an administrator disabled the ability for reviewers to add comments on the User Site.
Electronic signatures activated	Tracks the date and time that an administrator activated electronic signatures for document signoff on the User Site.
Electronic signatures deactivated	Tracks the date and time that an administrator deactivated electronic signatures for document signoff on the User Site.
Incident administrator added	Tracks the date and time that an administrator added an incident administrator.
Incident administrator deleted	Tracks the date and time that an administrator deleted an incident administrator.

Application — Administrative Option	Purpose
User created	Tracks the date and time that an administrator or user added a user account. This option tracks only the internal repository.
User modified	Tracks the date and time that an administrator or user modified a user account. This option tracks only the internal repository.
User deleted	Tracks the date and time that an administrator deleted a user account. This option tracks only the internal repository.
Permissions allowed/denied	Tracks the date and time that an administrator allowed or denied any permission to a user, group, or role.
Repository created	Tracks the date and time that an administrator added external repository information to VPC.
Repository modified	Tracks the date and time that an administrator modified external repository information in VPC.
Repository deleted	Tracks the date and time that an administrator deleted external repository information from VPC.
Repository sync started	Tracks the date and time that a synchronization between an external repository and VPC begins synchronization.
Repository sync success	Tracks the date and time that a synchronization between an external repository and VPC succeeds.
Repository sync failure	Tracks the date and time that a synchronization between an external repository and VPC fails.

Policy Document Option	Purpose
Policy documents created	Tracks the date and time that a user created a policy document.
Policy documents modified	Tracks the date and time that a user modified a policy document.
Policy documents modified in draft	Tracks the date and time that a user modified a policy document in Draft state.
Policy documents modified in review	Tracks the date and time that a user modified a policy document in Review state.
Policy documents modified in published	Tracks the date and time that a user modified a policy document in Published state.
Policy documents modified in archive	Tracks the date and time that a user modified a policy document in Archive state.
Policy document properties modified	Tracks the date and time that a user modified the properties of a policy document.
Policy documents deleted	Tracks the date and time that a user deleted a policy document from VPC.
Policy documents deleted from draft	Tracks the date and time that a user deleted a policy document from Draft state.
Policy documents deleted from archived	Tracks the date and time that a user deleted a policy document from Archived state.
Policy documents imported	Tracks the date and time that a user imported a policy document.
Policy documents copied	Tracks the date and time that a user copied a policy document.

Policy Document Option	Purpose
Policy documents copied from library	Tracks the date and time that a user copied a policy document from the library.
Policy documents copied from samples	Tracks the date and time that a user copied a policy document from the samples.
Policy documents copied from templates	Tracks the date and time that a user copied a policy document from the templates.
Policy documents copied from archive	Tracks the date and time that a user copied a policy document from Archive state.
Policy documents exported from library	Tracks the date and time that a user exported a policy document from the library.
Policy documents exported from samples	Tracks the date and time that a user exported a policy document from the samples.
Policy documents exported from templates	Tracks the date and time that a user exported a policy document from the templates.
Policy documents exported from draft	Tracks the date and time that a user exported a policy document from the Draft state.
Policy documents exported from review	Tracks the date and time that a user exported a policy document from the Review state.
Policy documents exported from published	Tracks the date and time that a user exported a policy document from the Published state.
Policy documents exported from archive	Tracks the date and time that a user exported a policy document from the Archive state.
Policy documents moved to review	Tracks the date and time that a user moved a policy document to the Review state.
Policy documents published	Tracks the date and time that a user moved a policy document to the Published state.
Policy documents archived	Tracks the date and time that a user moved a policy document to the Archive state.
Policy documents rejected from review	Tracks the date and time that a user rejected a policy document from the Review state.
Policy document ownership reassigned	Tracks the date and time that a user reassigned ownership of a policy document.
Comment added to policy documents in review	Tracks the date and time that a reviewer added a comment to a policy document in the Review state.
Comment added to published policy documents	Tracks the date and time that a user added a comment to a policy document in the Published state.
Comment deleted from policy documents in review	Tracks the date and time that a user deleted a comment from a policy document in the Review state.
Comment deleted from published policy documents	Tracks the date and time that a user deleted a comment from a policy document in the Published state.
Email sent for policy documents	Tracks the date and time that a user sent an email message from VPC regarding a policy document.
Documents acknowledged as reviewed	Tracks the date and time that a reviewer acknowledged reviewing a policy document.
Documents acknowledged as read	Tracks the date and time that a user acknowledged reading a policy document.
Documents electronically signed	Tracks the date and time that a user acknowledged reading a policy document by entering the password of the associated user ID.

Policy Document Option	Purpose
Language equivalent policy added	Tracks the date and time that a user adds a language equivalent copy of a policy document.
Language equivalent policy deleted	Tracks the date and time that a user deletes a language equivalent copy of a policy document.

Quiz Option	Purpose
Quizzes created	Tracks the date and time that a user created a quiz.
Quizzes modified	Tracks the date and time that a user modified a quiz.
Quizzes modified in draft	Tracks the date and time that a user modified a quiz in Draft state.
Quizzes modified in review	Tracks the date and time that a user modified a quiz in Review state.
Quizzes modified in published	Tracks the date and time that a user modified a quiz in Published state.
Quizzes modified in archive	Tracks the date and time that a user modified a quiz in Archive state.
Quizzes properties modified	Tracks the date and time that a user modified the properties of a quiz.
Quizzes deleted	Tracks the date and time that a user deleted a quiz from VPC.
Quizzes deleted from draft	Tracks the date and time that a user deleted a quiz from Draft state.
Quizzes deleted from archived	Tracks the date and time that a user deleted a quiz from Archived state.
Quizzes imported	Tracks the date and time that a user imported a quiz.
Quizzes copied	Tracks the date and time that a user copied a quiz.
Quizzes copied from samples	Tracks the date and time that a user copied a quiz from the samples.
Quizzes copied from archive	Tracks the date and time that a user copied a quiz from Archive state.
Quizzes exported from samples	Tracks the date and time that a user exported a quiz from the samples.
Quizzes exported from draft	Tracks the date and time that a user exported a quiz from the Draft state.
Quizzes exported from review	Tracks the date and time that a user exported a quiz from the Review state.
Quizzes exported from published	Tracks the date and time that a user exported a quiz from the Published state.
Quizzes exported from archive	Tracks the date and time that a user exported a quiz from the Archive state.
Quizzes moved to review	Tracks the date and time that a user moved a quiz to the Review state.
Quizzes published	Tracks the date and time that a user moved a quiz to the Published state.
Quizzes archived	Tracks the date and time that a user moved a quiz to the Archive state.
Quizzes rejected from review	Tracks the date and time that a user rejected a quiz from the Review state.

Quiz Option	Purpose
Quiz ownership reassigned	Tracks the date and time that a user reassigned ownership of a quiz.
Comment added to quizzes in review	Tracks the date and time that a reviewer added a comment to a quiz in the Review state.
Comment added to published quizzes	Tracks the date and time that a user added a comment to a quiz in the Published state.
Comment deleted from quizzes in review	Tracks the date and time that a user deleted a comment from a quiz in the Review state.
Comment deleted from published quizzes	Tracks the date and time that a user deleted a comment from a quiz in the Published state.
Email sent for quizzes	Tracks the date and time that a user sent an email message from VPC regarding a quiz.
Quizzes acknowledged as reviewed	Tracks the date and time that a reviewer acknowledged reviewing a quiz.
Quizzes taken	Tracks the date and time that a user completed a quiz on the VPC User Site.

Incident Option	Purpose
Incident reports created	Tracks the date and time that a user submits a security report within VPC.
Incident reports modified	Tracks the date and time that an administrator modifies a security report within VPC.
Incident reports deleted	Tracks the date and time that an administrator deletes an incident report from within VPC.
Incident report emails sent	Tracks the date and time that an administrator sent an email message from VPC regarding a security incident.

News Option	Purpose
News items created	Tracks the date and time that a user submits a news item.
News items modified	Tracks the date and time that a user modifies a news item.
News items deleted	Tracks the date and time that a user deletes a news item from within VPC.

Setting Logging Options

When you set up logging, you specify which actions you want VPC to log, and for each action, where you want to log the information. Use the following steps to set audit logging.

Note

For detailed information about each logging option, see “Understanding Logging Options.”

To set audit logging:

1. On the Administration tab, click **Options**.

   VPC displays the Options page with the Log tab on top.

2. Under **Active Events to Log**, click **Options**.

VPC displays the Logging Options page. Actions available for logging are grouped under categories by the type of action.

3. For each action that you want to track, click one or more of the check boxes next to the action to specify where VPC logs the data.

   Note
   To select the same logging location for all actions within a category, click the **Select *X*** check box, where ***X*** represents the logging location. for example, to log all actions under **Application — Access Options** to the VPC log file, click **Select File**.

4. Click **Submit** to save your audit choices.
5. Click **Cancel** to return to the Log tab.
6. Under **Audit File Path**, for **Path**, accept the default name and location for the log file or modify the data as appropriate.
7. Click **Update**.

Configuring VPC to Use a Mail Server

Setting a mail server in VPC allows document managers to send email messages to notify users to take action on policies and quizzes. VPC offers preconfigured, customizable messages for tasks such as:

- Notifying users when you post a policy or quiz for review
- Notifying users when you post a policy or quiz for reading
- Reminding non-compliant users to review a policy or complete a quiz

VPC offers several options to customize the way your organization uses the email notification feature. Use the following steps to set up your mail server and customize email notification.

Note
If VPC does not notify the specified users, verify that the **Originator Address** field contains a valid email address. If VPC does not send returned mail notification, verify the address. If VPC still does not send return notification, verify the document's access control list and the user account's correct group.

To set mail server information:

1. On the Administration tab, click **Options**, and then click **Mail**.
2. Type the URL of the mail server in the **Mail Server** field.
3. *Optional.* Type an email address in the **Originator Address** field as the email address to which VPC returns undeliverable email messages.

   Note
   VPC does not use this address in the **From** field when sending an email message. The mail server uses this address to report any undeliverable email messages. To automatically populate the **From** field, see Step 6.

4. *Optional*. Type the user ID required for mail server authentication in the **User ID** field and the associated password in the **Password** field.

5. *Optional.* Under **Automate E-mail Notification**, select when you want VPC to automatically display the E-Mail window. Document administrators use the E-Mail window to edit and send an email message when you post a document for review or publish to document.

   - **On Review** automatically displays the E-Mail window before you submit a document for review.
   - **On Publish** automatically displays the E-Mail window before you publish a document.

6. *Optional.* Click **Auto-populate the From Field with the sender's e-mail address** if you want VPC to automatically fill the **From** field of messages with the email address of the document author currently logged into the VPC Administration site. If you clear this option or if VPC does not know the email address of the document author, VPC uses the generic site administrator address.

7. *Optional.* If your user repository does not associate user IDs with an email address, select one or more of the **E-mail Recipient List Options**. If all options are clear, VPC cannot return a user email address list.

Note
For more information about user repositories, see "Understanding Deployment Options."

The information in the following table shows the different options available on the Mail Tab. The Mail Tab Fields column includes the fields selected on the Mail tab. The three other columns contain which area VPC verifies in the designated setup. For example, if you have **Build e-mail list from user ID/group name** and **Use groups for e-mail notification** selected, VPC sends a notice to the individual users with **Read** permissions and to the groups with **Read** permissions. Use the following table as a guide when setting your mail server.

Mail Tab Fields	Individual Users	DL Users	Groups
Build e-mail list from user ID/group name = ON Use single distribution list for everyone = OFF Use groups for e-mail notification = OFF	Yes	No	No
Build e-mail list from user ID/group name = OFF Use single distribution list for everyone = ON Use groups for e-mail notification = OFF	No	Yes	No
Build e-mail list from user ID/group name = OFF Use single distribution list for everyone = OFF Use groups for e-mail notification = ON	No	No	Yes
Build e-mail list from user ID/group name = ON Use single distribution list for everyone = OFF Use groups for e-mail notification = ON	Yes	No	Yes
Build e-mail list from user ID/group name = ON Use single distribution list for everyone = ON Use groups for e-mail notification = ON	No	Yes	No
Build e-mail list from user ID/group name = OFF Use single distribution list for everyone = OFF Use groups for e-mail notification = OFF	Yes	No	No

a. *Optional*. Click **Build e-mail list from user ID/group name**, and then type an entry in the **E-mail Suffix** field as the accepted company email address extension. For example, if all users have the email address format of `fname.lname@companyx.com`, type `@companyx.com` as a suffix.

b. *Optional*. Click **Use single distribution list for everyone**, and then type an email address in the **List name** field if a company-wide address exists, such as `all@companyx.com`.

c. *Optional*. Click **Use groups for e-mail notification** for VPC to notify users by their groups.

8. Click **Update**.

Changing the Browser Session Time Out

The default browser session time out for VigilEnt Policy Center is 30 minutes. After 30 minutes of inactivity, the browser prevents you from performing any action within VPC without logging on to VPC. Activity includes refreshing the browser and any communication with the server such as saving a document or settings on the Administration Site, and submitting answers to a quiz or acknowledging that you have read a policy document on the User Site. You can set the browser session time out for the Administration Site separately from the User Site. Use the following steps to change your browser session time-out period.

Note

Before changing the default browser session time out, verify that the maximum number of minutes that you are considering for each site within VPC is best for your organization. If the time-out minutes are more than necessary, the risk for a security incident increases if a user fails to log out before leaving a session of VPC unattended. However, if the time-out minutes are less than necessary, the browser may prevent your users from completing a quiz because the browser does not consider the action of clicking an answer within a quiz. Communication with the server occurs only when you click **Submit** upon quiz completion.

To change the browser session time out:

1. Open Windows Explorer.

2. ***If you want to change the Administration Site,*** navigate to **... NetIQ > VigilEnt Policy Center > server > webapps > VpcAdmin > WEB-INF**.

   If you want to change the User Site, navigate to **... NetIQ > VigilEnt Policy Center > server > webapps > policy > WEB-INF**.

3. Select `web.xml`, and then from the **Edit** menu select **Copy**.

4. Select the white space following `web.xml`, and then from the **Edit** menu select **Paste**.

   The computer creates a file named `Copy of web.xml`. This file is a backup of the `web.xml` file. You may delete this file after successfully changing the session time-out value.

5. Right-click `web.xml` and open the file in a text editor, such as Notepad

6. Select **Edit > Find**.

   The computer displays the Find dialog box.

7. Type the following text in the **Find what** field, and then click **Find Next**:

   ```
   <session-timeout>
   ```

8. Replace the default `30` with the number of minutes of inactivity before the browser times out the VPC Administration or User Site.

9. Select **File > Save**.
10. Restart the VigilEnt Policy Center service by accessing the Services window, selecting **VigilEnt Policy Center**, and then from the **Action** menu clicking **Start**.

Configuring the VPC Server for Document Access

VPC now allows you to configure browser window behavior and link generation components to streamline your workflows and processes.

Setting Browser Window Behavior

A standard means of alerting users to their need to comply with documents is to send them hyperlinks within an email message. When the links are accessed, VPC opens the document in the document viewer. A secondary window can also be opened to provide users the ability to peruse the User Site to determine if there are additional documents that need their attention. The default window behavior is to open two windows.

To set the browser window behavior for User Site Access links:

1. On the Administration tab, click **Options**, and then click **Document**.
2. Under the section titled User Site Access Links, select the appropriate option for controlling the number of windows VPC is to use in displaying documents.
3. Click **Update** to set the global configuration parameter for VPC.

Configuring Link Generation Components

To streamline the document link generation process, VPC allows you to configure the link creation components such as server, port, and protocol. Having preconfigured the settings, policy and quiz links are generated from a single VPC server specification standard allowing for consistency in appearance and accuracy in execution. During installation or upgrade to VPC, a default entry for the server specification is required.

To update the VPC Server Specification governing document link generation:

1. On the Administration tab, click **Options**, and then click **Document**.
2. Under the section titled VPC Server Specification, enter the URL users will adhere to when attempting to log on to the User Site.

   Note
   The URL should consist of the protocol (HTTP or HTTPS) in use, the VPC server name or IP, and the port. These components can vary based on whether you are configured to use IIS or Tomcat authentication. Be sure to test the link for accuracy before updating the server specification setting.

3. Click **Update** to set the global configuration parameter for VPC.

Configuring VPC Web Services

VPC offers web services that provide dynamic access to the business logic contained in the core VPC product so you can customize its delivery to applications and frameworks with which your users are more familiar, such as corporate portals and intranets. For more information about the services and possible use cases within your organization, see the *VPC Web Services Guide*. The following guidance pertains to the configuration of web services after they have been installed.

Note

Access to the Web Services tab is limited to users with the Configure VPC Web Services permission. For more information about permissions, see “Understanding Permissions.”

To access technical information for the offered web services:

1. On the Administration tab, click **Options**, and then click **Web Services**.
2. Click **Available Services** to view details regarding the services such as service descriptions and WSDL representations.
3. Click **Verify Connection** to test the uptime availability of the service connection.

To configure the security level for web service connections:

1. On the Administration tab, click **Options**, and then click **Web Services**.
2. Select the security level that is to govern connection authentication for the services.
3. If the Security Level selected is other than Level 1, proceed to the next section for determining the connection accounts.
4. If Level 1 is in use, click **Update** to save the security setting.

To set the connection accounts for VPC web services:

1. On the Administration tab, click **Options**, and then click **Web Services**.
2. In the connection account **Search** field, type the search criteria to search for the users or groups to associate with the connection privileges for the web services. VPC accepts wildcard characters such as asterisks (*).
   - To limit the search to only groups, click **Groups only search**.
   - To search for groups and users, click **Include groups in search**.
3. Click **Search**.
4. Select the users or groups you want to enable as connection accounts, and then click **>>** to move them to the Selected Users/Groups box.
5. Click **Update**.

Chapter 4

Setting the User Repository

A *user* is anyone with access to VPC. Organizations store users in one or more repositories and receive information and access based on the permissions set up for their user ID. You can configure VPC to use the users and groups stored in one or more LDAP-compliant databases, or create a separate set of users and store them in the VPC database.

User and group repository configuration depends on which source you select for your user database. For more information about user repository options, see "Understanding Deployment Options."

Using VPC as the User Repository

VPC defaults as your user repository after installation. When using VPC as your only repository, you can import user and group information from an outside source. Users exist in VigilEnt Policy Center as individuals and as group members. You can place users in groups based on a similar feature such as location, role, or responsibility within your organization.

When using VPC as the user repository, you need to maintain the data in two areas. Your users must remember two logon IDs and enter the information twice when accessing VPC sites. Most large organizations avoid duplicate user IDs and passwords by specifying an external source for the VPC user repository. However, if one of the external sources is not practical for your organization, use the procedures in this section to set up VPC as the user repository and populate the user database.

Setting VPC Password Options

When using VPC as the user repository, user authentication occurs within VPC when you provide a unique user ID and password.

Protecting a password is an easy way to prevent security breaches. Requiring users to create a password with multiple alphabetic and numeric characters and having a short expiration date helps decrease the chance of unauthorized access to VPC. Use the following steps to set the VPC password options.

To set password options:

1. On the Administration tab, click **Options**, and then click **Passwords**.

   VPC displays the Passwords tab.

2. Click the minimum number of characters in a password from the **Minimum VPC password length *X* characters** list, where ***X*** represents the minimum number.

3. *Optional*. Select the **Require at least one character which is NOT a letter** check box. VPC accepts only passwords with at least one numeric character.

4. *Optional*. Select the **Require at least one uppercase character** check box. VPC accepts only passwords with at least one uppercase character.
5. Set the life of the password by clicking one of the following options:
   - **Passwords never expire**.
   - **Passwords expire in *X* days** where ***X*** is a number between 1 and 999.
6. Click **Update**.

Importing a User List

Importing users provides an easy way to enter all users virtually without error. Use commas (,) to separate information for each user and use semi-colons (;) to separate users from each other. Because the data is so large when importing 500 or more users, we recommend that you perform this function after normal business hours. Use these steps to import an existing user list.

To import a user list:

1. On the Administration tab, click **Users**.

   VPC displays the User Info page.
2. Click **Import**.
3. Type the file path in the **File Name** field or click **Browse** to select the file.

   Separate users in this file by semi-colons, and separate each item within a user's record by commas. Use the following format:

   ```
   userID,password,firstname,lastname,email,department,extension
   ```

   If one of the variables does not exist, type the variable as a space. For example, if the data does not contain a user first name, use the following format:

   ```
   userID,password, ,lastname,email,department,extension
   ```
4. Click **Import** and verify that VPC properly imported the users by clicking **Search** on the User Info page.

Creating a User Account from the Administration Site

If you are using the internal repository, you can use VPC to create user accounts stored in the internal repository. You can create user IDs from the Administration Site or users can create their own IDs from the User Site. The following steps show how to create a user ID from the Administration Site.

Notes

- You can add users to a group while creating the user ID. For more information, see "Creating a User Group."
- If you are using Windows Active Directory for authentication or LDAP for your user repository, you cannot create a user group in VPC. Create your user groups through your Windows user manager utility.

To create a user account from the Administration Site:

1. On the Administration tab, click **Users**.

   VPC displays the User Info page.

2. Click **Add**.

   VPC displays the User page.

3. Type the user ID in the **User ID** field.
4. Type a password in the **Password** field and confirm by typing the same password in the **Confirm Password** field.
5. *Optional*. Type the information for inclusion in the VigilEnt Policy Center user profiles in the **First Name**, **Last Name**, **E-mail, Department**, and **Extension** fields.
6. *Optional*. Add the name of the user's manager by searching for and selecting the manager's user name in the **Search for Manager** area.
7. Click **Save** to add the new user and return to the User Info page.
8. Verify the user account by clicking **Search**.

Creating a User Group

A user group consists of users with a similar trait, such as the same department, title, or office. Assigning attributes to a group of users rather than to individual users saves time. Use these steps to create a user group.

Note
If you are using Windows Active Directory for authentication or LDAP for your user repository, you cannot create a user group in VPC. Create your user groups through your Windows user manager utility.

To create a user group:

1. On the Administration tab, click **Users**, and then click **Group Info**.

   VPC displays the Group Info page.

2. Click **Add**.
3. Type a name and description for the group in the **Name** and **Description** fields.
4. Click **Add** for either users or groups.

   VPC displays the search page.

5. In the **Search for Users** or **Search for Groups** field, type the name of the user or group account that you want to add to the group, and then click **Search**. You can search for all users or groups by clicking **Search** without making an entry in the **Search for Users** or **Search for Group** field.
6. Click the appropriate users or groups. To select more than one entry, press **CTRL**, and then click to select non-consecutive entries. Press **SHIFT**, and then click to select consecutive entries.
7. Click **Submit**.

   VPC displays the selection on the Group page.

8. Click **Save**.
9. Verify the current group list by clicking **Search**.

To add a user to an existing group during user ID creation:

1. Create a new user using the steps in “Creating a User Account from the Administration Site” on page 59, but instead of clicking **Save** to complete the process, click **Groups**.

   VPC displays the Group Membership dialog box with the existing groups in the **Available Groups** field.

2. Click the group to which you want to add the new user, and then click **>>** to move the group to the **Selected Groups** field.
3. Click **Close**, and then click **Save** in the User dialog box and VPC adds the user account to the appropriate group.

To add an existing group to a new group:

1. On the Administration tab, click **Users**, and then click **Group Info**.

   VPC displays the Group Info page.

   Note
   If you are creating a group to contain other groups, VPC displays all of the affected groups in the **Select Groups** field when you run a Policy Report or Quiz Report. For example, add a group named **Houston** to the ACL for a policy document. The **Houston** group contains a group named **Management**, but you did not assign **Management** to the document. Both **Houston** and **Management** are in the **Select Groups** field because the reports affect both of those groups.

2. Click **Add**.
3. Type a name and description in the **Name** and **Description** fields.
4. Click the second **Add** icon to add a new group.

   VPC displays the search page.

5. Type a group name in the **Search for Groups** field, and then click **Search**. You can search for all groups by clicking **Search** without making an entry in the **Search for Groups** field.
6. Click the appropriate group from the displayed list. To select more than one group, press **CTRL**, and then click to select non-consecutive groups. Press **SHIFT**, and then click to select consecutive groups.
7. Click **Submit**.

   VPC displays the selection on the Group page.

8. Click **Save** and verify the current group list by clicking **Search**.

Migrating Data to a User Account

You can migrate your user account data when a user changes user ID names for any reason, such as, a user gets married and changes their last name or when an organization changes user ID naming conventions. The migrate feature copies all compliance and access control list (ACL) data for a user ID and applies the information to another account. For this reason, do not use this feature to create new user IDs for different individual users.

To migrate data from an existing user account to a new user account:

1. On the Administration tab, click **Users**.

   VPC displays the User Info page.

2. In the **Search for Users** field, type the name of the new user account that you want to copy the data from an existing account, and then click **Search**. You can search for all users by clicking **Search** without making an entry in the **Search for Users** field.

3. Select the appropriate user account and click **Migrate**.

   VPC displays the Migration page. This page includes the **User ID**, **First Name**, and **Last Name** of the new user account.

4. In the **Existing User Account** field, type the name of the existing user account that you want to copy the data to the new user account, and then click **Search**. You can search for all users by clicking **Search** without making an entry in the **Existing User Account** field.

5. Click **Save** and VPC migrates the data to the selected user account.

Using an External User Repository

Most large organizations use an external user repository for increased speed, additional security, and reduced administration costs. Rather than importing the user data into VPC, you can access user and group data from Windows 2000 or later Active Directory.

Setting Active Directory as the User Repository

You can set VPC to access data in Active Directory through LDAP. VPC supports Active Directory only in a *native mode* domain as opposed to a *mixed mode* domain.

- In *native mode*, all domain controllers should run a Windows 2000 server or later, although other servers may run another Windows version.
- In *mixed mode*, some of the domain controllers may run Windows NT while client and member servers run another Windows version.

If you are using a mixed mode domain, use Windows NT for your user repository.

Notes

- You cannot change the user repository from Microsoft Windows NT to Active Directory. If you attempt to change the user repository from Windows NT, you cannot access any historical data and VPC provides inconsistent report results. The data still exists in the database, but you can only access the data directly from the database.
- The following procedure requires entries using Distinguished Name (DN) format. If you are unsure of how to enter the values using the correct syntax, see NetIQ knowledge base article NETIQKB36726.

To set Active Directory as the user repository:

1. On the Administration tab, click **Options**, and then click **Repository**.
2. On the Repository tab, click **Add**.

3. On the Repository Options page, type the name of the repository in the **Name** field. VPC does not accept the following characters in this field: `/ \ * ? < > |`

   Note
   Because VPC lists the repository name after every user and group name in *username@repositoryname* format, make the entry in this field 10 characters or less to avoid unnecessarily long identifiers.

4. *Optional.* Type the email address for the repository administrator in the **E-mail** field.
5. Click **My users are in an LDAP server**.
6. Expand **Field Mappings** and click **Active Directory** to set the default attribute mappings for Active Directory.

   Note
   To set attribute mappings other than the defaults, see "Setting Advanced LDAP Configuration."

7. Expand **LDAP Configuration**.
8. *Optional.* If you are using SSL, select the **Yes** check box.
9. For **LDAP URL**, type *one* of the following lines of data:
   - The location of the fully-qualified URL. Use the following format:

     `LDAP://<server name>:389`

     OR
   - The IP address of the server and the LDAP TCP port. Use the following format:

     `LDAP://192.168.72.1:389`

     Note
     The default LDAP TCP port is `389`. The default LDAP TCP Global Catalog port is `3268`.

10. For **Search Base**, type the name of the highest level that contains all users and groups you want to serve with VPC. Typically this is the domain name as identified in the following example: `dc=<domain name>,dc=com`.

    VPC uses the entry to search for user accounts. Specifying the highest folder level ensures that VPC finds all user accounts in the database.

11. Select the **Anonymous Bind** check box to connect to an LDAP server anonymously. Clear this check box to identify the connection. ***If you clear this check box***, VPC requires information in the **Bind DN** and **Password** fields.

    If you are using Microsoft Exchange, clear the **Anonymous Bind** field.

12. For **Bind DN**, type the full distinguished name of the account VPC uses when binding to the server. The account should have permissions to browse the entire contents of the Search Base and enumerate groups, for example:

    ```
    cn=Administrator,cn=Users,dc=<domain name>,dc=com
    ```

    Note
    If the value contains spaces, use quotation marks around the text, for example, `cn="policy admin",ou="san jose",dc=globalcorp,dc=com`.

13. For **Password**, type the password for the **Bind DN** account.
14. Click **Save**.

The following table shows an example of the settings used for an Active Directory server

Field	Value
My users are in an LDAP server	Yes
Use SSL	
LDAP URL	LDAP://hou007:389
Search Base	dc=globalcorp,dc=com
Anonymous Bind	

Bind DN	cn=Administrator,cn=Users,
	dc=globalcorp,dc=com

Password	********

Setting an LDAP Server Other than Active Directory as the User Repository

Using an LDAP-compliant server such as Novell eDirectory for the user repository may be possible in some customer environments, but *is not recommended or supported*. NetIQ Corporation strongly recommends using Active Directory and does not support setting an LDAP server other than Active Directory as the user repository. For more information about setting Active Directory as the user repository, see "Setting Active Directory as the User Repository" on page 39.

If you choose to set an LDAP server other than Active Directory as your user repository, complete the following steps.

Note
Verify that the user account connecting to LDAP has **Read** permission.

To use another LDAP server as the user repository:

1. On the Administration tab, click **Options**, and then click **Repository**.

   VPC displays the Repository tab.

2. Click **Add**.

   VPC displays the Repository Options page.

3. Type the name of the repository in the **Name** field. VPC does not accept the following characters in this field: `/ \ * ? < > |`

   Note
   Because VPC lists the repository name after every user and group name in *username@repositoryname* format, make the entry in this field 10 characters or less to avoid unnecessarily long identifiers.

4. *Optional*. Type the email address for the repository administrator in the **E-mail** field.

5. Click **My users are in an LDAP server**.

6. Expand **Field Mappings** and type the appropriate mapping information to set the attribute mappings for your repository. ***If you are using Microsoft Exchange 5.5 as your server***, click **Exchange**. ***If you are using Microsoft Exchange 2003 as your server***, click **Active Directory.**

   Note
   To set attribute mappings other than the defaults, see "Setting Advanced LDAP Configuration."

7. Expand **LDAP Configuration**.

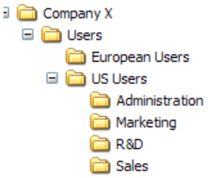
8. *Optional*. If you are using SSL, select the **Use SSL** check box.
9. In the **LDAP URL** field, type the location of the fully-qualified URL and port for the LDAP server. For example: `ldap://server_name:389`

Note
The default LDAP TCP port is `389`. The default LDAP TCP Global Catalog port is `3268`.

---

10. In the **Search Base** field, type the name of the top level group or folder used for searching user IDs. For example, `o=server_name.com`.

    When using Microsoft Exchange, the following table shows an example of a typical path for Microsoft Exchange.

Microsoft Exchange Folder Structure	If your user accounts are located in ...	The Search Base field should be ...
 Company X Users European Users US Users Administration Marketing R&D Sales	Company X	o=Company X
	Users	cn=Users,o=Company X
	US Users	cn=US Users, cn=Users,o=Company X

11. Select the **Anonymous Bind** check box to connect to an LDAP server anonymously. Clear this check box to identify the connection. ***If you clear this check box***, VPC requires information in the **Bind DN** and **Password** fields.

    If you are using Microsoft Exchange, clear the **Anonymous Bind** field.

12. ***If you clear the Anonymous Bind check box,*** type the logon information for LDAP in the **Bind DN** field. Use the full distinguished name of the account VPC uses when binding to the server, for example:

```
uid=admin,ou=admins,ou=server_name.com
```

Note
The **Bind DN** field should contain `cn=alias` when using a Microsoft Exchange server.

---

13. ***If you select the Anonymous Bind check box,*** do not use the **Bind DN** and **Password** fields. ***If you clear the Anonymous Bind check box,*** type the password used to log on to the LDAP server in the **Password** field.
14. Click **Save**. The following table shows an example of the settings used for an LDAP server.

Field	Value
My users are in an LDAP server	Yes
Use SSL	
LDAP URL	LDAP://hou007:370
Search Base	o=globalcorp.com
Anonymous Bind	Yes
Bind DN	
Password	

The following table shows an example of the settings used for a Microsoft Exchange server.

Field	Value
My users are in an LDAP server	Yes
Use SSL	
LDAP URL	
Search Base	o=GlobalCorp
Anonymous Bind	
Bind DN	cn=miou
Password	********

Setting Advanced LDAP Configuration

Different LDAP servers may require separate attribute name mappings from the defaults. If you have changed the attribute names for the objects VPC uses, you must adjust those mappings within VPC. Therefore, set VigilEnt Policy Center to look for data in the LDAP server using these specific names. This task is also necessary if you modify your LDAP server from its default settings. Use one of the following procedures to set LDAP server options.

Note

Using an LDAP-compliant server such as Novell eDirectory for the user repository may be possible in some customer environments, but *is not recommended or supported*. NetIQ Corporation strongly recommends using Active Directory and does not support setting an LDAP server other than Active Directory as the user repository.

To set attribute name mapping for a Microsoft Active Directory server:

1. On the Administration tab, click **Options**, and then click **Repository**.
2. Select the repository you want to address, and then click **Edit**.
3. Expand **Field Mappings**. To map attributes for individual IDs, continue with the next step. To map attributes for groups, skip to Step 10.
4. In the **User ID** field, type the attribute name used to uniquely identify a user in the LDAP server.
5. In the **User Password** field, type the attribute name used to hold a password.
6. Type the attribute names used to uniquely identify a person's **First Name** and **Last Name**.
7. Type the identifying attribute names in the **E-mail**, **Department**, and **Telephone** fields.
8. In the **Parent** field, type the attribute name representing the group to which the member belongs, such as: `memberOf`.
9. In the **User Object Class** field, type the attribute name used to identify the object class attribute value that identifies an LDAP object as a type of user.
10. In the **Group Name** field, type the attribute name used to uniquely identify the group name in the LDAP server.
11. In the **Description** field, type the attribute name for the description associated with the entered group name.
12. In the **Group Member** field, type the attribute name representing a member of the entered group.

13. In the **Parent** field, type the attribute name representing the group to which the member belongs, such as: `memberOf`.
14. In the **Object Class** field, type the attribute name used to identify the object class value. The object class value is unique to a group and used to distinguish a group object from a user object.
15. In the **Group Object Class** field, type the attribute name used to identify a unique object class, such as: `group`.
16. Click **Submit**.

To set attribute name mapping for LDAP:

1. On the Administration tab, click **Options**, and then click **Repository**.
2. Select the repository you want to address, and then click **Edit**.
3. Expand **Field Mappings**. To map attributes for individual user IDs, continue with the next step. To map attributes for groups, skip to Step 10.
4. In the **User ID** field, type the attribute name used to uniquely identify a user in the LDAP server.
5. In the **User Password** field, type the attribute name used to hold a password.
6. Type the attribute names used to identify a person's **First Name** and **Last Name**.
7. Type identifying attribute names in the **E-mail**, **Department**, and **Telephone** fields.
8. Verify that the **Parent** field is clear.
9. In the **User Object Class** field, type the attribute name used to identify the object class attribute value that identifies an LDAP object as a type of user.
10. In the **Group Name** field, type the attribute name used to uniquely identify the group name in the LDAP server.
11. In the **Description** field, type the attribute name for the description associated with the entered group name.
12. In the **Group Member** field, type the attribute name representing a member of the entered group.
13. Verify that the **Parent** field is clear.
14. In the **Object Class** field, type the attribute name used to identify the object class value. The object class value is unique to a group and used to distinguish a group object from a user object.
15. In the **Group Object Class** field, type the attribute name used to identify a unique object class.
16. Click **Submit**.

Notes

Verify the LDAP settings for the maximum number of search results returned. If the number of records requested is larger than the limit set by the server, which can occur when searching for users or viewing a report for a document with **Everyone Read** permission, the following results can occur:

- **LDAP:** Returns only the exact number requested. If there are more records than the allotted limit, they do not display.
- **Exchange**: Does not return any records. The entry in the **Maximum number of search results returned** field should exceed the number of records requested at any given time.

When setting VigilEnt Policy Center to use Microsoft Exchange as the user repository, use Microsoft IIS for authentication. When Exchange authenticates a user, Exchange uses a different user ID from the one used by the Microsoft Windows NT domain. Exchange maps the Windows NT domain user ID to its internal user ID. This action prevents VPC from directly authenticating users against Exchange alone.

To set attribute name mapping for a Microsoft Exchange server:

1. Set VigilEnt Policy Center to run under IIS as instructed in "Setting VPC to Run with an IIS Web Server." Be sure to use only the Windows NT challenge/response authentication, the integrated Windows authentication in Windows 2000 or 2003, for the policy and VpcAdmin virtual directories.
2. On the Administration tab, click **Options**, and then click **Repository**.
3. Select the repository you want to address, and then click **Edit**.
4. Expand **Field Mappings**.
5. ***If you are using Microsoft Exchange 5.5,*** click **Exchange**, and then skip to Step 17. ***If you are using Microsoft Exchange 2003,*** click **Active Directory**, and then skip to Step 17. To map attributes for individual IDs, continue with the next step. To map attributes for groups, skip to Step 11.
6. In the **User ID** field, type the attribute name used to uniquely identify a user in the LDAP server.
7. In the **User Password** field, type the attribute name used to hold a password.
8. Type the attribute names used to uniquely identify a person's **First Name** and **Last Name**.
9. Type additional identifying attribute names in the **E-mail**, **Department**, and **Telephone** fields.
10. In the **Parent** field, type the attribute name representing the group to which the member belongs, such as: `memberOf`.
11. In the **User Object Class** field, type the attribute name used to identify the object class attribute value that identifies an LDAP object as a type of user.
12. In the **Group Name** field, type the attribute name used to uniquely identify the group name in the LDAP server.
13. In the **Description** field, type the attribute name for the description associated with the entered group name.
14. In the **Group Member** field, type the attribute name representing a member of the entered group.
15. In the **Parent** field, type the attribute name representing the group to which the member belongs, such as: `memberOf`.

    Note
    Clear the **Parent** field if your assigned access control lists are not working properly AND VPC does not display the assigned groups for a user on the User Info page or display the assigned or nested groups for a parent group on the Group Info page.

16. In the **Object Class** field, type the attribute name used to identify the object class value. The object class value is unique to a group and used to distinguish a group object from a user object.
17. In the **Group Object Class** field, type the attribute name used to identify a unique object class, such as: `groupofnames`.
18. Click **Submit**.

Using Multiple External User Repositories

Some organizations have users and groups in multiple domains as a result of company mergers, global offices, or other factors. VPC allows you to access these domains by adding more than one external repository.

When you use multiple repositories, VPC continues to use the internal repository to store the VPC Administrator account. You cannot add users and groups from different repositories into a single group; however, you can use access control lists (ACLs) to manage these types of users and groups. For example, a document manager from a global corporation can send out a document to reviewers around the world by creating an ACL containing the reviewer and applying that ACL to the document. When the manager pushes the document out for review, all reviewers listed in the ACL receive the document regardless of the domain in which the user resides.

VPC avoids any confusion of duplicate users IDs by including the repository name with each user and group ID in the format *username@repositoryname* and *groupname@repositoryname*. For example, VPC displays “jsmith” in the repository named “Houston” as “jsmith@Houston” and “jsmith” in the repository named “Seattle” as “jsmith@Seattle.”

Synchronizing VPC with an External Repository

You must synchronize VPC regularly with your external repository for the most updated information about your users and groups. Note that VPC runs only one synchronization at a time. VPC must complete each synchronization before synchronizing with another repository. VPC displays the **Last Successful Sync** date and time along with the **Sync Duration** for each repository on the Repository Options page.

To synchronize VPC with an external repository:

1. Log on to the Administration Site.
2. On the Administration tab, click **Options**.
3. On the Options page, click **Repository**, and then click the name of the repository that you want to synchronize.
4. Click **Edit**.

   VPC displays the Repository Options page. The following table shows the available synchronization types and their scheduling options.

Synchronization Type	Scheduling Description
Now	Click **Run** and VPC begins synchronizing with the repository.
Once	Type a starting date and time, and then click **Save**. VPC begins synchronizing with the repository only once on the selected date and time.

Synchronization Type	Scheduling Description
By Minute	1. Type a number in the **Every *X* minute(s)** field, where *X* is the number of minutes between synchronizations. 2. Type a starting date and time. 3. Select one of the following end types: • **Run until cancelled** • **Run *X* times**, where *X* is the number of times VPC runs this synchronization • **Run until *mm/dd/yyyy***, where *mm/dd/yyyy* is the date when VPC stops running this synchronization 4. Click **Save**. VPC begins synchronizing with the repository every *X* minute(s) on the selected date and time.
Hourly	1. Type a number in the **Every *X* hour(s)** field, where *X* is the number of hours between synchronizations. 2. Type a starting date and time. 3. Select one of the following end types: • **Run until cancelled** • **Run *X* times**, where *X* is the number of times VPC runs this synchronization • **Run until *mm/dd/yyyy***, where *mm/dd/yyyy* is the date when VPC stops running this synchronization 4. Click **Save**. VPC begins synchronizing with the repository every *X* hour(s) on the selected date and time.
Daily	1. Type a number in the **Every *X* day(s)** field, where X is the number of hours between synchronizations. 2. Type a starting date and time. 3. Select one of the following end types: • **Run until cancelled** • **Run *X* times**, where *X* is the number of times VPC runs this synchronization • **Run until *mm/dd/yyyy***, where *mm/dd/yyyy* is the date when VPC stops running this synchronization 4. Click **Save**. VPC begins synchronizing with the repository every *X* day(s) on the selected date and time.

Synchronization Type	Scheduling Description
Weekly	1. Select a day in the **Every week on** area to run VPC on that day of the week. 2. Select a week in the **Week of the month** area to run VPC on that week of the month. 3. Type a starting date and time. 4. Select one of the following end types: • **Run until cancelled** • **Run *X* times**, where *X* is the number of times VPC runs this synchronization • **Run until *mm/dd/yyyy***, where *mm/dd/yyyy* is the date when VPC stops running this synchronization 5. Click **Save**. VPC begins synchronizing with the repository every *X* week(s) on the selected date and time.
Monthly	1. Select one of the following monthly selections: • **Day *X* of the month**, where *X* is the numbered day of the month • **The *X Y* of the month**, where *X* is the count of the corresponding *Y* entry, and *Y* is the day of the week 2. Select one or more months during which you want VPC to run the synchronization. 3. Type a starting date and time. 4. Select one of the following end types: • **Run until cancelled** • **Run *X* times**, where *X* is the number of times VPC runs this synchronization • **Run until *mm/dd/yyyy***, where *mm/dd/yyyy* is the date when VPC stops running this synchronization 5. Click **Save**. VPC begins synchronizing with the repository during the preferred month(s) on the selected date and time.
None	This synchronization type is the default. VPC does not synchronize with the repository until you select another synchronization type.

When you attempt to access the User Site through the IIS server, VPC does not display the logon page. VPC immediately authenticates your user account and provides access to the User Site Home Page.

Configuring IIS Authentication

If you are running Microsoft Windows with an IIS server, you can automatically authenticate your users without having them enter their logon credentials twice. Using IIS provides the following benefits:

- Additional security options, such as extra NTFS security and digital certificates
- Increased authentication response speed
- Synchronization with VPC, permitting the use of single user IDs and passwords

The following sections provide steps for configuring the IIS Web server in IIS 6.0 and 7.0. Complete the appropriate steps for your environment.

Configuring the IIS 6.0 Web Server for VPC

Microsoft Internet Information Server (IIS) authenticates users against the Windows domain account and that mechanism authenticates users. Complete the following steps to configure the IIS 6.0 Web server for VPC.

Note
In the following task, *`install_folder`* represents the folder where VigilEnt Policy Center resides. The default location is `C:\Program Files\NetIQ\VigilEnt Policy Center`.

To configure the IIS 6.0 Web server for VPC:

1. Locate the following file using Windows Explorer:

   `install_folder``\bin\iis\i386\tomcat_iis.reg`

   Note
   The installation folder contains two registry entry files. Ensure you select the `tomcat_iis.reg` file, otherwise.extraneous registry keys will be created.

2. Double-click the file to register the settings.

   The computer displays a verification message.

3. Click **Yes**.

   The registry initializes with a number of values needed by IIS to run the VigilEnt Policy Center server and VPC displays a verification message.

4. Click **OK**.

5. Open Internet Information Services (IIS) Manager and make the following additions:

Note
Verify that the virtual folder information is in the proper case. Be sure to capitalize `V` and `A` in `\VpcAdmin` in Step b.

   a. Create a virtual folder named `jakarta` on the default Web site and assign the following parameters:

      physical path: *`install_folder`*`\bin\iis\i386\`

      permissions: `execute`

   b. Create a virtual folder named `VpcAdmin` on the default Web site and assign the following parameters:

      physical path: *`install_folder`*`\server\webapps\VpcAdmin`

      permissions: `read`

      default documents: `index.html`

   c. Create a virtual folder named `policy` on the default Web site and assign the following parameters:

      physical path: *`install_folder`*`\server\webapps\policy`

      permissions: `read`

      default documents: `index.html`

   d. Add `install_folder\bin\iis\i386\isapi_redirector.dll` as an ISAPI filter on the Default Web Site and assign the name `jakarta`.

   e. Click `jakarta` and select **Properties** from the View menu.

      The jakarta Properties dialog box displays.

   f. Click **Directory Security**, and then click **Edit**.

   g. Clear the **Anonymous access** check box, and then click **OK**.

6. Add `jakarta` as a new Web service extension.

   a. In the Internet Information Services (IIS) Manager dialog box, select Web Service Extensions.

   b. In the Details pane, click **Add a new Web service extension**.

      The New Web Service Extension dialog box displays.

   c. For **Extension name**, type the name of the new Web service extension, `jakarta`.

   d. Click **Add**.

   e. For path to file, type the path or click **Browse** to navigate to *`install_folder`*`\bin\iis\i386\isapi_redirector.dll.`

   f. Click **OK** to add the file.

   g. Click **Set extension status to Allowed**.

   h. Click **OK** to create the new Web service extension.

7. Restart the IISAdmin service.

8. Restart the World Wide Web Publishing service.

   You can now access the Administration Site and User Site through the default Web site port (80) instead of through port 8080, that is, `//localhost/VpcAdmin` instead of `//localhost:8080/VpcAdmin`.

Configuring the IIS 7.0 Web Server for VPC

Using VPC with Internet Information Services (IIS) 7.0 Web Server on a Windows Server 2008 computer requires some additional configuration steps to enable access to the Administration Site and the User Site. Whether you have a new VPC installation or are upgrading an existing installation, perform these steps on the IIS Web Server computer after you install or upgrade VPC.

Before you begin configuring IIS 7.0, verify you have the IIS 6 Management Compatibility Components installed to ensure the equivalent configurable options are available to configure IIS 7.0 for your VPC environment. If you do not have these components installed, you may need to reference your Windows installation disk.

Notes

- In the following procedure, *`install_folder`* represents the folder where VigilEnt Policy Center resides. The default location is `C:\Program Files\NetIQ\VigilEnt Policy Center`.
- Windows 2008 can be installed in either 32-bit mode or 64-bit mode. The following procedure includes steps for both modes. The steps are slightly different, so ensure you complete the appropriate steps for your environment.

To configure the IIS 7.0 Web server for VPC:

1. ***If the server is running on Windows 2008 in 32-bit mode,*** locate the following file using Windows Explorer:

   `install_folder``\bin\iis\i386\tomcat_iis.reg`

2. ***If the server is running on Windows 2008 in 64-bit mode,*** locate the following file using Windows Explorer:

   `install_folder``\bin\iis\i386\tomcat_iisWoW64.reg`

   Note

   The installation folder contains two registry entry files. Ensure you select the appropriate registry entry file for 32-bit or 64-bit mode, otherwise.extraneous registry keys will be created.

3. Double-click the file to register the settings.

4. Click **Yes** to confirm. The registry initializes with a number of values needed by IIS to run the VigilEnt Policy Center server, and then VPC displays a verification message.

5. Open Internet Information Services (IIS) Manager.

6. Perform the following steps to add the jakarta application:

   a. In the left pane, expand **Sites** and then right-click **Default Web Site** and select **Add Application**.

   b. In the **Alias** field, type `jakarta`.

   c. In the **Physical path** field, type *`install_folder`*`\bin\iis\i386\`.

d. In the left pane, select the **jakarta** application to display the configurable options in the center pane.

e. In the center pane under IIS, double-click the **Handler Mappings** icon.

f. In the right pane under Actions, click **Edit Feature Permissions**.

g. Verify the **Read**, **Script**, and **Execute** permissions are selected and click **OK**.

h. In the left pane, select the **jakarta** application.

i. In the center pane under IIS, double-click the **Authentication** icon.

j. Right-click the **Anonymous Authentication** option and select **Disable**.

k. Right-click the **Windows Authentication** option and select **Enable**.

7. Perform the following steps to add the VPC Administration Site:

a. In the left pane, right-click **Default Web Site** and select **Add Virtual Directory**.

b. In the **Alias** field, type `VpcAdmin`. This value is case-sensitive, so ensure you capitalize `V` and `A` in `VpcAdmin`.

c. In the **Physical path** field, type *`install_folder`*`\server\webapps\VpcAdmin`. The name of the directory is case-sensitive, so ensure you capitalize `V` and `A` in `VpcAdmin`.

d. In the left pane, select the **VpcAdmin** directory to display the configurable options in the center pane.

e. In the center pane under IIS, double-click the **Handler Mappings** icon.

f. In the right pane under Actions, click **Edit Feature Permissions**.

g. Verify the **Read** and **Script** permissions are selected and click **OK**.

h. In the left pane, select the **VpcAdmin** directory.

i. In the center pane under IIS, double-click the **Authentication** icon.

j. Right-click the **Anonymous Authentication** option and select **Disable**.

k. Right-click the **Windows Authentication** option and select **Enable**.

8. Perform the following steps to add the VPC User Site:

a. In the left pane, right-click **Default Web Site** and select **Add Virtual Directory**.

b. In the **Alias** field, type `policy`.

c. In the **Physical path** field, type *`install_folder`*`\server\webapps\policy`.

d. In the left pane, select the **policy** directory to display the configurable options in the center pane.

e. In the center pane under IIS, double-click the **Handler Mappings** icon.

f. In the right pane under Actions, click **Edit Feature Permissions**.

g. Verify the **Read** and **Script** permissions are selected and click **OK**.

h. In the left pane, select the **policy** directory.

i. In the center pane under IIS, double-click the **Authentication** icon.

j. Right-click the **Anonymous Authentication** option and select **Disable**.

k. Right-click the **Windows Authentication** option and select **Enable**.

9. Perform the following steps to add the Isapi filter:

a. In the left pane, select **Default Web Site**.

b. In the center pane under IIS, double-click the **ISAPI Filters** icon.

c. In the right pane under Actions, click **Add**.

d. In the **Filter name** field, type `Jakarta`.

e. In the **Executable** field, type *`install_folder`*`\bin\iis\i386\isapi_redirector.dll`.

10. Perform the following steps to add the Isapi filter to the main server:

a. In the left pane, select the main server. This server should have the same name as the computer, such as *`ServerName Home`*.

b. In the center pane, double-click the **ISAPI and CGI Restrictions** icon.

c. In the right pane under Actions, click **Add**.

d. In the **ISAPI or CGI path** field, type *`install_folder`*`\bin\iis\i386\isapi_redirector.dll.`

e. In the **Description** field, type `Jakarta`.

f. Verify the **Allow extension path to execute** option is selected.

g. Click **OK** to create the new Web service extension.

11. ***If the server is running on Windows 2008 in 64-bit mode,*** perform the following additional steps in Internet Information Services (IIS) Manager to enable 32-bit compatibility:

a. In the left pane under the name of the server, select **Application Pools**.

b. In the Actions right pane, click the **Set Application Pool Defaults** link.

c. In the Application Pool Defaults window, expand **General**.

d. Select **Enable 32-Bit Applications** and select **True** in the list.

e. Click **OK**.

12. Restart the IISAdmin service.

13. Restart the World Wide Web Publishing service.

You can now access the Administration Site and User Site through the default Web site port (80) instead of through port 8080, that is, `//localhost/VpcAdmin` instead of `//localhost:8080/VpcAdmin`.

Enabling Automatic User Authentication Through IIS

Once you have configured Microsoft IIS support, you can set VPC to authenticate users through the Web server. This feature lets users who are authenticated against the Windows domain directly connect to the User Site without logging on again. Use the following steps to configure IIS for automatic authentication. Be sure to perform the steps in VPC as well as on the IIS server.

Note
This function works only with Microsoft Internet Explorer 6.0 or later.

To enable automatic user authentication through IIS:

1. Complete the following steps on the IIS server:

   a. Open the Internet Information Services (IIS) Manager.

   b. Click **policy**, and then click **Properties** from the View menu.

   The computer displays the Policy Properties dialog box.

   c. Click **Directory Security**, and then, under **Authentication and access control**, click **Edit**.

   The computer displays the Authentication Methods dialog box.

   d. Click **Enable anonymous access**.

   e. Click **Integrated Windows authentication**.

   f. Click **OK** to close the Authentication Methods dialog box.

   g. Click **OK** to close the policy Properties dialog box, and then repeat these steps substituting the **VpcAdmin** folder for the **policy** folder.

2. Complete the following steps in VPC:

   a. Log on to the Administration Site.

   b. On the Administration tab, click **Options**.

   VPC displays the Options page.

   c. Click **Authentication**, and then click **I want to use my web server authentication mechanism**.

   d. Click **Update**.

When you attempt to access the User Site through the IIS server, VPC does not display the logon page. VPC immediately authenticates your user account and provides access to the User Site Home Page.

Chapter 5

Controlling User Access

VigilEnt Policy Center provides significant flexibility in controlling user access to administrator functions and policy documents. Careful planning of user access configuration prevents granting or denying access accidentally. A well-planned configuration helps reduce security events and increases productivity. By default, only administrators have the power to assign permissions.

Using Roles

A role is a title or responsibility that can contain assigned permissions. You can place roles on an individual user ID or group of user IDs. This flexible feature allows an administrator to assign responsibility to a type of user, such as a manager, and apply permissions based on function within the organization.

VigilEnt Policy Center comes with the following built-in roles:

- The Auditor role has permissions to the functions used to view reporting and manage audit logging.
- The Compliance Manager role has permissions to create and manage reports on all documents.
- The Power User role has permissions to the functions used to manage policy documents and quizzes and run compliance reports.
- The VPC Administrator role has permissions to every function within VPC.

Adding a User or Group to an Existing Role

You can quickly assign permissions to a user or group by adding them to a role.

To add a user or group to an existing role:

1. On the Administration tab, click **Users**, and then click **Role Info**.

   VPC displays the Role Info page.

2. In the **Search for Roles** field, type the name of the role to which you want to add a user or group, and then click **Search**.

   VPC displays the list of roles matching the entered criteria.

3. Select the role to which you want to add a user or group, and then click the **Edit** icon.

   VPC displays the Role dialog box.

4. Click one of the **Add** icons to add either a user or group to the displayed role.

VPC displays the search page.

5. Type a user name in the **Search for Users** or **Search for Groups** field, and then click **Search**. You can search for all users by clicking **Search** without making an entry in the search field.
6. Click the appropriate users or groups from the displayed list. To select more than one entry, press **CTRL**, and then click to select non-consecutive entries. Press **SHIFT**, and then click to select consecutive entries.
7. Click **Submit**.

   VPC displays the Role dialog box and the users or groups selected for the role.
8. Click **Save**.

Creating a New User Role

In addition to the two default roles, you can create new roles that correspond to the job descriptions in your organization. Use the following steps to create a user role.

To create a user role:

1. On the Administration tab, click **Users**, and then click **Role Info**.

   VPC displays the Role Info page.
2. Verify that the role that you want to add does not already exist in VPC by typing the role name in the **Search for Roles** field, and then clicking **Search**. You can search for all roles by clicking **Search** without making an entry in the **Search for Roles** field.
3. Click **Add**.

   VPC displays the Role page.
4. Type a **Role Name** and **Description**.
5. Click one of the **Add** buttons to add either a user or group to the displayed role.

   VPC displays the search page.
6. Type a user name in the **Search for Users** or **Search for Groups** field, and then click **Search**. You can search for all users by clicking **Search** without making an entry in the search field.
7. Click the appropriate users or groups from the displayed list. To select more than one entry, press **CTRL**, and then click to select non-consecutive entries. Press **SHIFT**, and then click to select consecutive entries.
8. Click **Submit**.

   VPC displays the selection in the Role page.
9. Click **Save**.
10. Verify the current role list by clicking **Search**.

Managing User Access to VPC

Permissions grant or deny access to a specific feature in VPC. VPC allows you to define custom roles and modify the permissions of each role to match your access requirements.

Understanding Permissions

VigilEnt Policy Center provides significant flexibility in managing the roles and permissions of your users. For example, you can create a role called Backup Administrator that has only those permissions necessary to modify the user repository settings on the VPC Administration Site. Another example is to create a role called Content Editor that is restricted to creating VPC policy documents and quizzes. You can apply permissions to a specific role, user group, or individual user.

Note
Specifying VPC permissions on a role gives only those users in that specific role the right to take actions, such as editing documents, within VigilEnt Policy Center. Users with document creation permissions can create their own documents, but cannot create documents for other users to edit unless they are re-assigned ownership or given specific permissions. Apply restrictions on individual documents by using access control lists.

Caution
Because this feature is complex, before performing this function be sure to review all options and plan the features you want to allow or deny to each role, user, or group.

Reporting Permissions

The reporting permissions control access to the following types of reports available in VPC:

Incident Reporting

Used to alert staff of threats and to track violations as they occur. An efficient Information Security department resolves issues and helps create a safer, more secure environment within the organization by learning from report results.

Compliance Reporting

Used to create, manage, and view reports within VPC. Some permissions depend on other permissions to work correctly. For example, a user who is responsible for deleting reports must have the Delete Reports permission along with the View Reports permission to access the View tab or the Archive Reports permission to view the Archive tab.

The following table shows the available report permissions and their use.

Permissions	Use
Reporting	Controls access to all subsequent reporting functions, including security incident, user, quiz, group, and policy document reporting.
Reporting > **Incident Reporting**	Controls access to all subsequent security incident reporting functions, including modifying, viewing, searching, and adding reports.
Reporting > Incident Reporting > **View Audit Reports for Incidents**	Controls viewing of any auditing reports for security incidents.
Reporting > Incident Reporting > **Modify Incident Reports**	Controls modification of any security incident report.
Reporting > Incident Reporting > **View Incident Reports**	Controls viewing of any security incident report.
Reporting > Incident Reporting > **Search Incident Reports**	Controls searching for any security incident report.
Reporting > Incident Report > **Add Incident Reports**	Controls adding a security incident report.

Permissions	Use
Reporting > **Compliance Reporting (Global)**	Controls access to documents used in reporting.
Reporting > **Compliance Reporting (Global) > Create Reports**	Controls access to the Configure tab in compliance Reporting and allows the user to create policy, quiz, and user reports.
Reporting > **Compliance Reporting (Global) > Create Reports > Quiz Reports**	Controls the ability of the user to create quiz reports.
Reporting > **Compliance Reporting (Global) > Create Reports > Policy Reports**	Controls the ability of the user to create policy document reports.
Reporting > **Compliance Reporting (Global) > User Reports**	Controls the ability of the user to create user reports.
Reporting > **Compliance Reporting (Global) > Delete Reports**	Controls the ability of the user to delete reports. Users with this permission also must have the **View Reports** permission to access the View tab and the **Archive Reports** permission to access the Archive tab.
Reporting > **Compliance Reporting (Global) > View Reports**	Controls access to the View tab in Compliance Reporting and allows the user to view all reports.
Reporting > **Compliance Reporting (Global) > Set ACLs on Stored Reports**	Controls the ability of the user to manage the access control list (ACL) for available reports. Users with this permission also must have the **View Reports** permission to access the View tab and the **Archive Reports** permission to access the Archive tab.
Reporting > **Compliance Reporting (Global) > Archive Reports**	Controls access to the Archive tab in Compliance Reporting.

Administration Permissions

The administration permissions control access to the following types of administrative responsibilities available in VPC:

User/Group/Role Management

Used to manage the permissions for each user, user group, and user roles within an organization. Rather than have thousands of users that are considered individual entities granted permissions separately, you can add users to groups or assign users to roles. For example, once assigned to groups and roles within VPC, 1,000 users may be divided into only 10 groups and seven roles, and an administrator can grant permissions to those few categories rather than to each user.

Admin Reports

Used to run administration reports that show high-level information about ACLs, documents, and the VPC license.

Options

Used to manage many functions within VigilEnt Policy Center, such as license key updates, tracking, mail service, and database configuration and user repository controls.

Incident Reporting

Used to manage how your users report threats and violations and what information VPC gathers as an incident occurs. This information includes the security incident type, current status, any required action, and also controls the security administrator information within VPC.

User Site Administration

Used to manage the display and use of the VPC User Site. An organization has control over the available options, permissions, and the look of the User Site.

Edit ACLs

Used to manage who can access an item based on the assigned access control lists (ACLs). Administrators use ACLs to manage user access to a specific policy document, quiz, or news item.

Edit Permissions

Used to manage who can allow or deny permissions to users. This permissions administrator can affect only those permissions to which the administrator has access. For example, if an administrator has access to all incident reporting permissions, only then can they affect those permissions. However, if the administrator does not have permissions on the content permissions, this administrator cannot affect a user's content permissions.

The following table shows the available administration permissions and their use.

Permissions	Use
Administration	Controls access to all subsequent administration functions, including user, group, and role management, options, security incident reporting, permissions, news items, and quizzes.
Administration > **User/Group/Role Management**	Controls access to all subsequent user, group, and role management functions.
Administration > User/Group/Role Management > **Manage Roles**	Controls adding, changing, and deleting user roles.
Administration > User/Group/Role Management > **Manage Groups**	Controls adding, changing, and deleting user groups.
Administration > User/Group/Role Management > **Manage Users**	Controls adding, changing, and deleting user accounts.
Administration > **Admin Reports**	Controls access to the administration reports.
Administration > Admin Reports > **Audit Reports**	Controls access to the audit reports.
Administration > Admin Reports > Audit Reports > **View Quiz Audit Reports**	Controls viewing quiz audit reports.
Administration > Admin Reports > Audit Reports > **View Policy Document Audit Reports**	Controls viewing policy document audit reports.
Administration > Admin Reports > Audit Reports > **View User Audit Reports**	Controls viewing user audit reports.
Administration > Admin Reports > Audit Reports > **View Incident Audit Reports**	Controls viewing incident audit reports.
Administration > Admin Reports > Audit Reports > **View News Audit Reports**	Controls viewing news item audit reports.
Administration > Admin Reports > Audit Reports > **View Application Audit Reports**	Controls viewing application audit reports.
Administration > Admin Reports > **Document Reports**	Controls access to the document reports.
Administration > Admin Reports > **License Reports**	Controls access to the VPC license reports.
Administration > Admin Reports > **ACL Reports**	Controls access to the access control list reports.

Permissions	Use
Administration > **Options**	Controls access to all subsequent options, including managing audit logging, license keys, password policy, document tracking data, VM options, mail options, company information, database configuration options, and your user repository.
Administration > Options > **Manage Logging**	Controls changing logging parameters.
Administration > Options > Manage Logging > **Select Log Destination**	Controls changing the audit log destination.
Administration > Options > Manage Logging > **Enable Site Diagnostics for Troubleshooting**	Controls changing site diagnostics.
Administration > Options > Manage Logging > **Enable Audit Logging**	Controls changing audit logging enablement.
Administration > Options > Manage Logging > **Select Audit Event Options**	Controls changing event parameters.
Administration > Options > Configure VPC Web Services	Controls changing the configuration details for VPC Web Services.
Administration > Options > **Change License Key**	Controls changing the license key.
Administration > Options > **Change Password Policy**	Controls changing the password policy setup.
Administration > Options > **Change Document Options**	Controls changing the policy document setup.
Administration > Options > **Import Digital Certificates**	Controls importing digital certificates into VPC
Administration > Options > **Delete Policy Document and Quiz Tracking Data**	Controls deleting the policy document and quiz tracking data.
Administration > Options > **Change VM Options**	Controls changing options on the VM tab in VPC.
Administration > Options > Manage Policy Languages	Controls changing the language preferences for policies.
Administration > Options > **Change Mail Options**	Controls changing email options.
Administration > Options > **Change Company Information**	Controls changing the company name and security officer’s name within VPC.
Administration > Options > **Set Database Configuration Options**	Controls setting database configuration options.
Administration > Options > **Change Authentication Options**	Controls changing user authentication options.
Administration > Options > **Change User Repository**	Controls changing the user repository.
Administration > **Incident Reporting**	Controls access to all subsequent security incident reporting functions, including adding and deleting incident types, status, administrators, and required actions, and editing existing security administrator information.
Administration > Incident Reporting > **Add Incident Types**	Controls adding an incident type to the security incident reporting options.
Administration > Incident Reporting > **Add Status**	Controls adding a status to the security incident reporting options.

Permissions	Use
Administration > Incident Reporting > **Delete Status**	Controls deleting a status from the security incident reporting options.
Administration > Incident Reporting > **Delete Incident Types**	Controls deleting an incident type from the security incident reporting options.
Administration > Incident Reporting > **Delete Action Required**	Controls deleting a required action from the security incident reporting options.
Administration > Incident Reporting > **Add Incident Administrators**	Controls adding a security administrator.
Administration > Incident Reporting > **Edit Incident Administrator Information**	Controls editing security administrator information.
Administration > Incident Reporting > **Delete Incident Administrators**	Controls deleting security administrator names.
Administration > Incident Reporting > **Add Action Required**	Controls adding a required action to the security incident reporting options.
Administration > **User Site Administration**	Controls access to all subsequent User Site administration functions, including setting User Site permissions, managing policy information options, and customizing the User Site.
Administration > User Site Administration > **Set User Site Privileges**	Controls setting permissions on the VPC User Site.
Administration > User Site Administration > **Policy Information Options**	Controls setting options on the User Site, including receiving comments, document approval text, and document display order.
Administration > User Site Administration > **Customize User Site**	Controls the customization of the VPC User Site.
Administration > **Edit ACLs**	Controls access to policy documents, quizzes, and news items.
Administration > **Edit Permissions**	Controls changing the permissions throughout VPC.

Content Permissions

The content permissions control access to the following types of content available in VPC:

Policy Document

Used to manage the creation and use of policy documents within VPC. The policy document permissions are divided between management permissions and end-user permissions. Management permissions include creating a document, moving the document through the different phases within VPC, and controlling reporting. Like quizzes, a user reads, and then acknowledges receipt of the document, and may review the document beforehand.

News Items

Used to manage the creation and use of news items within VPC. An administrator can use news items to immediately alert users of important information, such as warning users of an email message virus or reminding users of a planned server outage for maintenance.

Quiz

Used to manage the creation and use of quizzes within VPC. The quiz permissions are divided between management permissions and end-user permissions. Management permissions include creating a quiz, moving the quiz through the different phases within VPC, and controlling reporting. As with policy documents, a user reads, and then completes the quiz and may review the quiz beforehand.

Manage Folders

Used to manage the creation and use of folders within VPC. You can create folders to contain all policy documents and quizzes pertaining to a particular subject or event, such as a folder named “Cyberterrorism” that includes all related documents. If an organization wants to review coverage of the topic of cyberterrorism, an administrator can access the specific folder and view the reports for the related documents.

The following table shows the available content permissions and their use.

Permissions	Use
Content	Controls access to all subsequent content functions, including policy documents, news items, and quizzes.
Content > **Policy Document**	Controls access to all subsequent policy document functions, including management and end-user permissions.
Content > Policy Document > **Management Permissions**	Controls access to all subsequent management permissions options, including Vulnerability Manager, document state management and editing, viewing status and log validation for your documents, and generating reports.
Content > Policy Document > Management Permissions > **Compliance Reports for Policy Documents**	Controls access to the Compliance Reporting tab.
Content > Policy Document > Management Permissions > Compliance Reports for Policy Documents > **Create Reports for Policy Documents**	Controls the ability to create reports on documents for which the user has Manage privileges.
Content > Policy Document > Management Permissions > Compliance Reports for Policy Documents > Create Reports for Policy Documents > **Policy Reports for Policy Documents**	Controls the ability to create policy reports on documents for which the user has Manage privileges.
Content > Policy Document > Management Permissions > Compliance Reports for Policy Documents > Create Reports for Policy Documents > **User Reports for Policy Documents**	Controls the ability to create user reports on documents for which the user has Manage privileges.
Content > Policy Document > Management Permissions > Compliance Reports for Policy Documents > **Delete Reports for Policy Documents**	Controls the ability of the user to delete reports. Users with this permission also must have the **View Reports for Policy Documents** permission to access the View tab and the **Archive Reports for Policy Documents** permission to access the Archive tab.
Content > Policy Document > Management Permissions > Compliance Reports for Policy Documents > **View Reports for Policy Documents**	Controls access to the View tab in Compliance Reporting and allows the user to view all reports on documents for which the user has Manage privileges.
Content > Policy Document > Management Permissions > Compliance Reports for Policy Documents > **Archive Reports for Policy Documents**	Controls access to the Archive tab in Compliance Reporting and allows the user to view all reports on documents for which the user has Manage privileges.
Content > Policy Document > Management Permissions > **VM**	Controls access to all subsequent Vulnerability Manager options, including sending documents to VM, viewing VM controls on documents, and creating VM inspections for documents.
Content > Policy Document > Management Permissions > VM > **Send Policy Documents to VM**	Controls sending a policy document containing controls to VM.

Permissions	Use
Content > Policy Document > Management Permissions > VM > **View VM Controls on Policy Documents**	Controls viewing VM controls on policy documents
Content > Policy Document > Management Permissions > VM > **Create VM Inspections for Policy Documents**	Controls creating VM checks to verify controls on policy documents.
Content > Policy Document > Management Permissions > **State Management**	Controls access to all subsequent state management permissions for policy documents including sending documents to draft, review, archived, or published phase and approval of policy documents.
Content > Policy Document > Management Permissions > State Management > **Send Policy Documents to Draft**	Controls sending policy documents to the draft phase.
Content > Policy Document > Management Permissions > State Management > **Send Policy Documents to Review**	Controls sending policy documents to the review phase.
Content > Policy Document > Management Permissions > State Management > **Send Policy Documents to Archived**	Controls sending policy documents to the archived phase.
Content > Policy Document > Management Permissions > State Management > **Send Policy Documents to Published**	Controls sending policy documents to the published phase.
Content > Policy Document > Management Permissions > **Document Editing**	Controls access to all subsequent document editing options, including importing, creating, exporting, editing, deleting, and copying policy documents.
Content > Policy Document > Management Permissions > Document Editing > **Import Policy Documents**	Controls importing policy documents.
Content > Policy Document > Management Permissions > Document Editing > **Create Policy Documents**	Controls creating policy documents.
Content > Policy Document > Management Permissions > Document Editing > **Export Policy Documents**	Controls exporting policy documents.
Content > Policy Document > Management Permissions > Document Editing > **Edit Policy Documents**	Controls editing policy documents.
Content > Policy Document > Management Permissions > Document Editing > **Delete Policy Documents**	Controls deleting policy documents.
Content > Policy Document > Management Permissions > Document Editing > **Copy Policy Documents**	Controls copying policy documents.
Content > Policy Document > Management Permissions > **View Comments/Status on Policy Documents**	Controls viewing the comments added to or the current status of policy documents.
Content > Policy Document > Management Permissions > **View Audit Reports for Policy Documents**	Controls viewing the audit reports for policy documents.

Permissions	Use
Content > Policy Document > Management Permissions > **Generate Reports for Policy Documents**	Controls policy document report generation.
Content > Policy Document > Management Permissions > **View the Log Validation for Policy Documents**	Controls viewing log validation for policy documents.
Content > Policy Document > Management Permissions > **Set ACLs on Policy Documents**	Controls setting access controls lists (ACLs) on policy documents.
Content > Policy Document > Management Permissions > **Reassign Policy Documents**	Controls reassigning the responsibility of policy documents to another user or administrator.
Content > Policy Document > Management Permissions > **Add/ Remove Policy Documents to Folders**	Controls adding and removing policy documents within folders.
Content > Policy Document > **End User Permissions**	Controls access to all subsequent user permission options, including reading, acknowledging, and reviewing policy documents.
Content > Policy Document > End User Permissions > **Read Policy Documents: Acknowledgement Not Required**	Controls reading policy documents without requiring an acknowledgement that you read the document.
Content > Policy Document > End User Permissions > **Read Policy Documents: Acknowledgement Required**	Controls reading policy documents and requires an acknowledgement that you read the document.
Content > Policy Document > End User Permissions > **Review Policy Documents**	Controls reviewing policy documents.
Content > **News Items**	Controls access to all subsequent new item options, including managing and viewing new items.
Content > News Items > **Manage News Items**	Controls managing news items.
Content > News Items > **View News Items**	Controls viewing news items.
Content > News Items > **View Audit Reports for News Items**	Controls viewing the audit reports for news items.
Content > **Quiz**	Controls access to all subsequent quiz options, including management and end-user permissions.
Content > Quiz > **Management Permissions**	Controls access to all subsequent management permissions, including document editing, quiz state management, viewing quiz log validation, folder management, quiz reports, viewing comments and status of quizzes, reassigning quizzes, and setting access control lists on quizzes.
Content > Quiz > Management Permissions > **Compliance Reports for Quizzes**	Controls access to the Compliance Reporting tab.
Content > Quiz > Management Permissions > Compliance Reports for Quizzes > **Create Reports for Quizzes**	Controls the ability to create reports on quizzes for which the user has Manage privileges.
Content > Quiz > Management Permissions > Compliance Reports for Quizzes > Create Reports for Quizzes > **User Reports for Quizzes**	Controls the ability to create user reports on quizzes for which the user has Manage privileges.

Permissions	Use
Content > Quiz > Management Permissions > Compliance Reports for Quizzes > Create Reports for Quizzes > **Policy Reports for Quizzes**	Controls the ability to create quiz reports on quizzes for which the user has Manage privileges.
Content > Quiz > Management Permissions > Compliance Reports for Quizzes > **Delete Reports for Quizzes**	Controls the ability of the user to delete reports. Users with this permission also must have the **View Reports for Quizzes** permission to access the View tab and the **Archive Reports for Quizzes** permission to access the Archive tab.
Content > Quiz > Management Permissions > Compliance Reports for Quizzes > **View Reports for Quizzes**	Controls access to the View tab in Compliance Reporting and allows the user to view all reports on quizzes for which the user has Manage privileges.
Content > Quiz > Management Permissions > Compliance Reports for Quizzes > **Archive Reports for Quizzes**	Controls access to the Archive tab in Compliance Reporting and allows the user to view all reports on documents for which the user has Manage privileges.
Content > Quiz > Management Permissions > **Document Editing**	Controls access to all subsequent policy document editing options, including importing, copying, creating, exporting, deleting, and editing quizzes.
Content > Quiz > Management Permissions > Document Editing > **Import Quizzes**	Controls importing quizzes into VPC.
Content > Quiz > Management Permissions > Document Editing > **Copy Quizzes**	Controls copying quizzes.
Content > Quiz > Management Permissions > Document Editing > **Create Quizzes**	Controls creating quizzes.
Content > Quiz > Management Permissions > Document Editing > **Export Quizzes**	Controls exporting quizzes.
Content > Quiz > Management Permissions > Document Editing > **Delete Quizzes**	Controls deleting quizzes.
Content > Quiz > Management Permissions > Document Editing > **Edit Quizzes**	Controls editing quizzes.
Content > Quiz > Management Permissions > **State Management**	Controls access to all subsequent state management permissions for quizzes including sending quizzes to published, review, draft, or archived phase and approval of quizzes.
Content > Quiz > Management Permissions > State Management > **Send Quizzes to Published**	Controls sending quizzes to the published phase.
Content > Quiz > Management Permissions > State Management > **Send Quizzes to Review**	Controls sending quizzes to the review phase.
Content > Quiz > Management Permissions > State Management > **Send Quizzes to Draft**	Controls sending quizzes to the draft phase.
Content > Quiz > Management Permissions > State Management > **Send Quizzes to Archived**	Controls sending quizzes to the archived phase.
Content > Quiz > Management Permissions > **View the Log Validation for Quizzes**	Controls viewing log validation for quizzes.

Permissions	Use
Content > Quiz > Management Permissions > **Add/Remove Quizzes to Folders**	Controls adding and removing quizzes within folders.
Content > Quiz > Management Permissions > **Generate Reports for Quizzes**	Controls quiz report generation.
Content > Quiz > Management Permissions > **View Comments/Status on Quizzes**	Controls viewing the comments added to or the current status of quizzes.
Content > Quiz > Management Permissions > **View Audit Reports for Quizzes**	Controls viewing the audit reports for quizzes.
Content > Quiz > Management Permissions > **Reassign Quizzes**	Controls reassigning the responsibility of quizzes to another user or administrator.
Content > Quiz > Management Permissions > **Set ACLs on Quizzes**	Controls setting access controls lists (ACLs) on quizzes.
Content > Quiz > **End User Permissions**	Controls access to all subsequent user permissions, including reviewing and reading quizzes.
Content > Quiz > End User Permissions > **Review Quizzes**	Controls reviewing quizzes.
Content > Quiz > End User Permissions > **Read Quizzes: Acknowledgement Required**	Controls reading quizzes and requires and acknowledgement that you completed the quiz.
Content > **Manage Folders**	Controls folder creation and management.

Granting Permissions for a Role, User, or Group

You can allow or deny permissions to a role, user, or group. When granting permissions, you can take many paths. One path is to allow only those permissions that are necessary for a role, user, or group to function. Use the following steps to allow or deny permissions.

To allow permissions for a role, user, or group:

1. On the Administration tab, click **Permissions**.
2. Select the appropriate name from the **Role/User/Group** list.
3. Click either **Allow** or **Deny**, and then select the check box next to each appropriate permission.
4. Click **Update** when you have finished.

Creating a Backup Administrator Account

A backup administrator account is useful if the functions of an administrator are needed but the administrator is unavailable. A backup administrator account also protects the supplied administrator account. Because of the power of the administrator account in general, use the backup administrator account only when the primary account is unavailable. This example includes creating a role, adding users, and then adding permissions. Use the following steps to create a backup administrator account.

To create a backup administrator role:

1. On the Administration tab, click **Users**, and then click **Role Info**.
2. On the Role Info tab, click **Add**.

VPC displays the Role dialog box.

3. Type `Backup VPC Administrators` in the **Role Name** field.
4. Type `Protection for VPC Admin Role` in the **Description** field.
5. Click one of the **Add** icons to add a new user or group.
6. In the **Search for Users** or **Search for Groups** field, type the name of the account that you want to add to the role, and then click **Search**. You can search for all users or groups by clicking **Search** without making an entry in the search field.
7. Click the appropriate entry from the displayed list. To select more than one entry, press **CTRL**, and then click to select non-consecutive entries. Press **SHIFT**, and then click to select consecutive entries.
8. Click **Submit**.

   VPC displays the selected users.
9. Verify that the Role dialog box displays the correct users, and then click **Save**.
10. Verify that VPC created the role by clicking **Search** with a clear **Search for Roles** field.

To add permissions to the backup administrator role:

1. On the Administration tab, click **Permissions**, and then select **Backup VPC Administrators** from the **Role/User/Group** field.

   The Permissions page displays the current permissions for the VPC Administrator.
2. Select the **All Permissions** check box, and then click **Update**.

   VPC displays a verification message.
3. Click **OK**.

Managing User Access to Documents

An access control list (ACL) is a named set of privileges for a group of users to access the content in VigilEnt Policy Center. Document managers associate ACLs with a document to control who can see the document and what they can do with it.

Understanding Access Control Lists (ACLs)

An ACL associates users with access privileges. You apply ACLs to documents to control the level of access to the document. An ACL can include one or more of the following access privileges:

Required to Read (RR)

Requires users to acknowledge that they have read a specific document. VPC displays the document in the User Site Home page until the user acknowledges that they have read the document.

Read but Not Required (NR)

Permits users to read a published document, but does not require proof that the reader read the document. Use this option if you want a public domain document available for users to read, but do not require that your users read the document.

Review (RV)

Permits users to review a document in the review phase.

Manage - Admin Site (M)

Permits document owners, who have the proper permissions, to access the Administration site to make changes to the content of a document.

VPC offers the following ways to create and associate ACLs:

- Preconfigure a set of ACLs and later associate them with documents. For more information, see “Creating an Access Control List” and “Applying an Existing ACL to a Policy Document.”
- Create a unique ACL for the document when you create, review, or publish a document. For more information, see “Applying User Permissions Directly to a Policy Document.”

Note
While an ACL applies privileges to users, a user group consists of users with a similar trait and is used to assign attributes to a group of users rather than to individual users. Because of this distinction, you should not use ACLs within VPC for large numbers of users. Groups of users numbering 1,000 or more should be addressed within your repository and not within VPC. ACLs for over 1,000 users cause poor performance issues when using VPC.

Creating an Access Control List

A user may need only a certain type of access to a policy document or quiz on the VPC User Site. For example, a user may not need access to review a policy document, but does need Read access. Creating ACLs allows you to specify who can perform what actions. Document managers can then apply the necessary ACLs to the documents.

Once you create an access control list, you can designate the privilege for new users or groups when adding them to the list. Perform the following steps to create a new ACL.

To create an access control list:

1. On the Administration tab, click **ACL**.

   VPC displays the ACL page.

2. Click **Add**.
3. Type a name for the type of access in the **ACL Title** field.
4. Select one or more access privilege. For descriptions of each access privilege, see “Understanding Access Control Lists (ACLs).”

   Note
   If you have multiple power users who may edit a specific document, assign the **Manage** privilege to each user or VPC allows edits by only one user. Assign the **Manage** privilege to only users who are power users and have access to the Administration Site.

5. In the **Search** field, type the search criteria to search for the users or groups to associate with the access privileges selected in Step 4. VPC accepts wildcard characters such as asterisks (*).
   - To limit the search to only groups, click **Groups only search**.
   - To search for groups and users, click **Include groups in search**.
6. Click **Search**.

VPC displays the available users or groups in the **Available Users/Groups** box.

7. Select the users or groups that you want to have access to the document, and then click **>>** to move them to the **Selected Users/Groups** box.
8. *Optional.* Under **Apply ACL to Documents**, select the documents to which you want to apply the ACL, and then click **>>** to move them to the **Selected Documents** box.
9. Click **Save**.

Setting the Default Access Control List

VPC allows you to select an access control list that applies to all new documents. If you select the **Everyone Read** ACL, VPC displays every subsequently-published document on the Home Page of the User Site for all users. Use the following procedure to set the default ACL.

To set a default access control list:

1. On the Administration tab, click **ACL**.

   VPC displays the ACL page.
2. Click **Options**.

   VPC displays the Options dialog box.
3. Select the appropriate ACL from the **Default ACL** list, and then select **Apply selected default ACL to new items**.
4. Click **Update**.

Excluding Document Authors from Acknowledge Requirements

VPC requires document authors to read and acknowledge the documents they publish. VPC enforces this requirement even if the assigned ACL allows everyone to read the policy document without acknowledgement. Use the following procedure to modify ACLs so that policy authors do not have to read or acknowledge the policies they create.

To exclude document authors from acknowledge requirements:

1. On the Administration tab, click **ACL**.

   VPC displays the ACL page.
2. Click **Include hidden ACLs**.
3. Scroll through the list of ACLs and select an ACL in the format `owner_userid`, where `userid` corresponds to the user who created the document. VPC adds these ACLs to the list when an administrator creates a policy document or quiz.
4. Click **Edit**.

   VPC displays the ACL page for the selected ACL.
5. Locate the name of the document author under **Selected Users/Groups**.

   Notice that the author has all available permissions: M, RV, RR, and NR.

6. Select the name of the document author and click **<<** to move the user from the **Selected Users/ Groups** list to the **Available Users/Groups** list.

Note
Reapply the author to the document or the author loses access to the document. Until you reapply the owner to the document, only the Site Administrator can access the document.

7. Under **Set the Access Privileges**, click **Manage – Admin Site**.
8. Click **Search** to populate the **Available Users/Groups** box.
9. Under **Available Users/Groups**, select the name of the document author, and then click **>>** to move the name to the **Selected Users/Groups** box.
10. Click **Save**.
11. Repeat Step 2 through Step 10 for each of the other ACLs in the format `owner_userid.`

Setting Access Control List Automation

You can set VPC to automatically prompt to set access control for a document before an administrator submits a document for review or publishes a document. This feature allows you to include ACL management as part of the document workflow. Use the following procedure to set ACL automation.

Note
You can also set VPC to automatically display the E-Mail window before an administrator submits a document for review or publishes a document. For more information, see “Configuring VPC to Use a Mail Server.”.

To set ACL automation:

1. On the Administration tab, click **Options**, and then click **Document**.
2. Under **Automate ACL Management**, click on of the following options for when you want VPC to display the Manage Access Control for a Document dialog box:
   - **On Review** automatically displays the Manage Access Control for a Document window before you submit a document for review.
   - **On Publish** automatically displays the Manage Access Control for a Document window before you publish a document.
3. Click **Update**.

Chapter 6

Preparing for Document Management

The key to a successful deployment of VigilEnt Policy Center is managing VPC documents. Before you begin using VPC, set standards for the format and content of your policies and develop a naming scheme and file structure for storing policies. If your policies are in HTML, consider how to manage the graphics in your policies. This chapter provides planning and configuration information to help you maximize the benefits of using VPC.

Planning and Setting Standards

VPC can manage documents in a variety of file formats. It is important to understand the characteristics of each file type so that you can select the format that offers the most advantages for your organization.

Understanding Document File Types

VPC supports documents that are in VPC internal XML format, HTML, DOC, DOCX, PDF, and RTF file format. The following topics describe some of the specifics of working with each file type.

VPC Internal XML (XML)

When you use the VPC Policy Editor and Quiz Editor, VPC creates the document using an internal XML file format. This type of format allows you to:

- Add commentary and user examples to your documents
- Use library documents

The internal XML format is versatile, but not as flexible as some of the other formats because of the structured format. You have limited control over the formatting of the documents when the User Site displays these files. Because of this limitation, perform any edits to an XML file using the editor in VPC.

HyperText Markup Language (HTML)

VPC includes an HTML Policy Editor that allows you to create and edit policies in HTML format. This file type gives you complete control when formatting documents. Also, with the native HTML support, you can create HTML documents by cutting and pasting from documents in other file formats. This method is efficient for users who want to import large amounts of existing information.

Microsoft Word (DOC/DOCX) and Rich Text Format (RTF)

If you are familiar with Microsoft Word, you may want to use the Microsoft Word Editor feature in VPC. This feature allows you to use many of the functions available in MS Word when creating and editing your policy documents. You can also import a DOC, DOCX, or RTF file, and then edit your document using the editor.

Ensure user computers meet all requirements to work with Microsoft Word documents in VPC. For more information, see "Microsoft Word Document Requirements" on page 14.

Adobe PDF (PDF)

VPC does not provide an editor for PDF files. However, you can import existing security policies that are in Adobe Acrobat PDF format. VPC treats these files like any other documents, with the following exceptions:

- Documents imported from PDF are read-only. You cannot edit the files from within VigilEnt Policy Center.
- The search function on the VPC User Site does not search the content of the imported documents. However, when importing, you can associate "keywords" that display in a document search.
- Users should have Adobe Acrobat or Adobe Reader on their computer to view the policy.

Determining Which File Type to Use

When choosing the best document file type to use for your organization, base your decision on both short-term and long-term considerations. First, consider the file type of your existing policies. Next consider the abilities of each file type. If your existing policies are in a different file type than the one you select, you can import the files and then convert them as you edit. The following table compares each file type on important aspects of document management.

Feature	XML	HTML	DOC/ DOCX	PDF
Automatic Keyword indexing	X	X		
Flexible formatting		X	X	X
Ability to create documents outside of VPC		X	X	X
Ability to edit documents in VPC	X	X	X	
WYSIWYG editor		X	X	X
Ability to include header and footer			X	X
Increased usability	X	X		
Reduced administrator overhead	X	X	X	
Ability to track changes			X	X

Setting Language Preferences

Understanding the language preferences of the intended audience for policies is crucial to the success of any policy program. Often users are asked to read policies in languages that are not their primary language, resulting in confusion or frustration on the part of the reader, or worse, compliance with a policy they did not fully understand. VPC offers the ability to define the primary site language as well as upload language equivalent copies of policies so that readers can view the policy in their desired language.

To set the language preferences for VPC:

1. On the Administration tab, click **Options**, and then click the Languages tab.
2. To determine the Primary Site Language, select the desired language from the dropdown box.

   This language serves as the default language preference when policies and their translated titles do not match the language specification in the browser.

   Note
   The list of available languages for the primary site designation is limited to the languages that are currently supported in the VPC User Site interface.

3. To set Available Policy Languages, select the check boxes associated with the languages to be offered for equivalency uploads.

   Note
   The list of available languages for the equivalency uploads is broader than what is currently supported for the interface text languages. While the limitation remains for the interface language, users can view the actual policy in the native language, assuming policy creators have provided the translated copy of the policy.

4. Click **Update** to save the changes to the language preferences.

Setting Policy Standards

Security policy documents are important for audits and legal dispute resolution. Correctly written and implemented, policy documents act as a clear statement of management intentions, reducing potential liability. It is important for your organization to set standards to ensure that policies are consistent and provide the content required for the purpose of your organization. It is important to set a standard for the sections and content of each policy document.

After your organization agrees on a standard format, you can create document templates to enforce those standards. For more information about creating policy templates, see “Working with Document Templates.”

Managing HTML Policy Documents

If you choose to use HTML as your policy document file type, additional considerations are required to ensure that your documents display and print properly.

Note
Vector Markup Language (VML) is not supported in the editor. HTML documents imported from Microsoft Word must be saved as **“Web Page, Filtered (*.htm, *.html)”** prior to importing them into VPC.

Managing Images in HTML Policy Documents

VPC supports including images in HTML document. When you create a document using a VPC policy editor, VPC provides an option to include the image, and then uploads the image file to the VPC server and automatically references the correct path when a user views the document.

When you import files with images, all hyperlinks to hosted files or files accessible through HTTP protocol remain intact on import. However, if the links are relative to the location of the files on your computer, you can specify the image files during the import process so that VPC can upload them to the server and reference the correct path.

The following topics are recommended best practices for managing images in HTML documents:

- Host all files that you use across the enterprise, such as corporate logos and standard corporate images, outside of VPC and access them through HTTP protocol. This practice avoids the need to upload the same image files to VPC multiple times, and therefore reduces the demand for disk space on the VPC server.
- Ensure adequate hard drive capacities to handle uploading files to the VPC server. For companies over 1000 users, we recommend two 18GB RAID-configured SCSI hard drives. This should be more than sufficient at the outset; however, monitor the drive periodically to make sure adequate space exists.
- Set a size restriction for files you want to upload to VPC that is compatible with your environment. By default, VPC enforces a maximum size restriction of 20MB or 20971520 bytes. You can change the default value by modifying the `MAX_FILE_UPLOAD_SIZE` value in the Properties table of the VPC database. However, based on your environment and the memory allotted to VPC, you may encounter performance issues when importing if you set the maximum value too high.

Setting VPC to Print a PDF Version of an HTML Policy

Documents created in HTML format often lose their formatting when printed. You can set VPC so that when a user prints an HTML document from the Document Reader Window of the User Site, a PDF version of the document prints instead of the HTML document.

Use the following rules to ensure that the PDF version prints:

- Name the PDF file the exact same name as the policy with a PDF extension. For example, if the policy name is **E-mail Usage Policy**, name the PDF file `Email Usage Policy.pdf`.
- Store the PDF versions of the document in the folder that you specify when you set this option.

To set VPC to print a PDF version of an HTML document:

1. On the Administration tab, click **Options**, and then click **Document**.
2. Under **Printable Version**, click **Use the PDF version of a document as the printable version of HTML policy documents**.
3. For **PDF Directory URL**, type the full path to the folder containing the PDF versions of the HTML policies.
4. Click **Update**.

Organizing Documents

You can create folders in VPC to store similar policy documents and quizzes in a single location. NetIQ Corporation recommends developing a folder structure and naming scheme before you begin importing and creating documents. Typical schemes include organizing policies by business unit, location, department, subject, or a combination of these groups.

VPC provides custom fields to set sort properties for a document. Sort properties control the order in which the User Site displays documents and allow you to reduce the number of folders required to store documents. If you select to use sort properties, NetIQ Corporation recommends that you plan and set up a scheme before you begin managing policies. When document managers import and create policies, they can enter values into the sort property fields.

Creating Folders

You can create a folder from either the Policy Center tab or the Education tab and store both policy documents and quizzes in the folder. You can add documents and quizzes in draft, review, or published phase to a folder, but cannot add archived quizzes. Use one of the following procedures to create folders.

To create a folder from the Policy Center tab:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. Click **Manage Folders**.

   VPC displays the Folder Editor dialog box.

3. Click **Add Subfolder**.

   VPC displays the new folder field.

4. Type the name for the folder, such as `Data Classification`, and then click **Save**.

5. Click **Close** to return to the View/Edit Policy page.

To create a folder from the Education tab:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. Click **Folders**.

   VPC displays the Folder page.

3. Click **Subfolder**.

   Note
   You can use a folder created on the Policy Center tab for organizing your quizzes. If you are updating VPC, all quizzes previously not assigned to a folder are assigned to the root folder during the update.

   VPC displays the new folder field.

4. Type the name for the folder, such as `Data Classification`, and then click **Save**.

5. Click **Close** to return to the View/Edit Quiz page.

Setting Sort Properties for Policy Documents

Creating a sort property adds a custom field to the properties page of a document. When a document manager enters a value in the field, VPC uses the value to group and sort policies in the User Site. For example, you can create a property called Cyberterrorism and add a **Property Type** of **Integer**. Document managers can use this field to sort how the documents display by entering `1` for the document to display at the top of the list of cyberterrorism policies, `2` for the second document in the list, and so forth. Use the following steps to manage the sort properties of a policy document.

Note
You may receive an error if you click **Cancel** while in the Policy Property Editor dialog box. If this error occurs, resolve the error by following the steps in "Increasing Your Temporary Internet Disk Space."

To set policy document sort properties:

1. On the Administration tab, click **Options**, and then click the Document tab.
2. Click **Create**.
3. In the **Name** field, type a descriptive name for the property. For example, if you want to sort your documents about physical security, you can type `Physical Security`. Or, if you are creating a custom property containing a list of departments in your organization, you can type `Dept.` VPC allows you to filter on this property when you configure a Master Document Report.
4. In the **Description** field, type a description of the property. For example, if you typed `Physical Security` in the **Name** field, type `Physical Security Sorting` in the **Description** field.
5. In the **Type** field, select the type associated with the property you are creating. VPC offers the following types:
   - **Text**: VigilEnt Policy Center displays documents using a particular **Property Name** in order based on alphabetical characters, such as `A`, `B`, and `C`. If you skip a letter, VPC displays the document containing the next letter in the series. For example, if no documents contain the letter `B` as a property, VPC displays the documents in the order `A`, `C`, and `D`.
   - **Integer**: VigilEnt Policy Center displays documents using a particular **Property Name** in order based on numerical characters, such as `1`, `2`, and `3`. If you skip a letter, VPC displays the document containing the next number in the series. For example, if no documents contain the number `2` as a property, VPC displays the documents in the order `1`, `3`, and `4`.
   - **Floating Point**: VigilEnt Policy Center displays documents using a particular **Property Name** in order based on alphanumerical characters, such as `A`, `B`, and `C`; `1`, `2`, and `3`, and based on decimal location. For example, VPC displays your documents in the order `2.1.1`, `2.1.2`, and `2.1.3`. If you have a document with a property of `2.2`, VPC displays this document after all of the `2.1` documents. If you skip a letter or number, VPC displays the document containing the next letter or number in the series. For example, if no documents contain the number `2.1.2` as a property, VPC displays the documents in the order `2.1.1`, `2.1.3`, and `2.1.4`.
   - **List**: The List type allows you to enter a custom list of items to be used in creating and searching for policy documents. By creating a standard list of items for policy owners to select from, you can ensure terminology is consistent across your organization, and policy searches are more productive. For example, you might use this custom property to specify the departments in your organization, such as `IT`, `HR`, `MKT`, `R&D`, and `Sales`.
6. ***If you selected the List property type***, enter each list item in the **Entry** field. VPC displays items in alphabetical order.
7. Under Usage Parameters, specify whether you want the custom property to be visible on all documents. If you select **Yes**, policy owners must complete this field when creating a policy.

8. Under Usage Parameters, specify whether you want the custom property to be required to be available for searching. The default value is **No**. If you select **Yes**, policy owners cannot change this value when creating a policy.

9. Click **Add** and VPC displays the property that you have created in the **Custom Properties** area. The list displays the properties beginning with the most recently-added.

Chapter 7
Developing Policy Documents

VPC offers several ways to create policy documents. In addition to using one of the editors in VPC, you can create policy documents from samples and templates. You can also create policies outside of VPC and then import them into VPC. Once policies exist in VPC, you can use a policy editor to modify and update the policy.

Procedures for creating, importing, and editing policy documents depend on the document file type your organization uses. For more information about document file types, see "Understanding Document File Types."

Developing VPC Internal XML Policy Documents

The VPC Policy Editor creates and edits documents using an internal XML format. The editor guides you through creating each section of a policy, and you can easily insert statements from the document library or from other published documents.

Understanding the Parts of a VPC Internal XML Policy Document

VPC internal XML policy documents typically include six basic components. These components help you create standardized policies that define roles and responsibilities, make employees aware of required procedures, and act as clear statements of management intentions. The following table shows the basic parts of a VPC policy document.

Title	Use
Preface Note	A preface note provides more details about the document. The note resides at the beginning of the policy document following the title. Use this field to store a version number or effective date.
Category	Categories help define a policy document. Many categories exist to address separate issues within a document. For example, categories may include an executive summary, scope of the document, and roles and responsibilities.
Subcategory	Subcategories help further define categories.
Statement	Statements provide the detailed definition and classification for the category. You can add a statement to any category or subcategory.
Related Document	A related document is any published policy document that shares an attribute such as regulation or topic. Use this link to relate a document to an earlier version.
Post Note	A post note con contain final details about the document. The note resides at the end of the policy document. Use this field to store a version number or effective date.

Creating a VPC Internal XML Policy Document

Using the VPC Policy Editor to create a document provides flexibility in development because you can easily insert statements from the document library or from other published documents. Use the following steps to create a policy document using the VPC Policy Editor.

Notes

- By default, policy documents are available for one year from the creation date. You can change the document availability by adjusting the **Available From** and **Available To** dates in the Properties window for the document.
- For more information about the sections of a policy document, see "Understanding the Parts of a VPC Internal XML Policy."

To create a VPC internal XML policy document:

1. On the Policy Center tab, click **New Policy**.

   VPC displays the New Policy page.

2. Click **Policy Editor**.

   VPC displays the Policy Editor page.

3. Click **VPC Policy Editor**, and then click **Submit**.

   VPC displays the Edit page.

4. Type the document's title in the **Title** field and the author's name in the **Author** field.
5. Add the appropriate document components.

   Note
   As you create the document, click **View** to see the final document.

6. Click **Save**, and then click **OK**.

To add a preface note:

You can add a preface note to a document, category, subcategory, or statement using the item's editor. For example, you can add a preface note to a category by clicking **Edit** to the right of the category name and clicking **Preface Note**.

1. On the Edit page, click **Preface Note**.

   VPC displays two new fields. You can add any type of information to these fields.

2. In the first field, type the subject information, such as a note title.
3. In the second field, type descriptive text, such as the document purpose.
4. Click **Save**, and then click **OK**.

To add a category:

You can move categories and subcategories up one place at a time when editing a document. Click **Move** to the right of the category or subcategory that you want to move, and then VPC moves the category or subcategory up one place. Click again to move up another place.

1. On the Edit page, click **Category**.

   VPC displays a New Category box.

2. Click **Edit** to the right of the field.

   VPC displays the Category Detail dialog box.

3. In the **Title** field, type the new category for example `Using An Email Account Assigned To Someone Else`.

4. *Optional.* Click **Preface Note** to add a note to the category.

5. In the **Description** field, type a description for the new category, such as information about the necessity for email account usage.

6. *Optional.* Click **Post Note** to add a note to the category.

7. Click **Save** and VPC displays the new category name within the policy document.

To add a subcategory:

1. On the Edit page, under the appropriate category, click **Subcategory**.

   VPC displays a New Category box under the category.

2. Click **Edit** to the right of the field.

   VPC displays the Category Detail dialog box.

3. In the **Title** field, type the new subcategory, for example `Interoffice Memo`.

4. *Optional.* Click **Preface Note** to add a note to the subcategory.

5. In the **Description** field, type description for the new subcategory, such as information about protecting interoffice memos.

6. *Optional.* Click **Post Note** to add a note to the subcategory.

7. Click **Save** and VPC displays the new subcategory name within the policy document.

To add a statement:

1. On the Edit page, under the appropriate category, click **Statement**.

   VPC displays the statement box following the category or subcategory area.

2. ***If you want to create only a statement,*** simply type the explanatory information or policy statement. ***If you want to create a statement with more detail,*** continue with the next step.

3. Click **Edit** to the right of the field.

   VPC displays the Edit Detail dialog box.

4. In the **Title**, **Text**, and **Commentary** fields, type the details for the new statement.

5. *Optional.* Click **Preface Note** to add a note to the statement.

6. *Optional.* Click **Post Note** to add a note to the statement.

7. *Optional*. Click **Example** to add example text to the statement.

8. Click **Save** and VPC displays the new statement within the policy document.

To add text from a library policy:

1. On the Edit page, under the appropriate category, click **From Library**.

   VPC displays the Source Documents dialog box.

2. Click the library you want to use.

   VPC displays the Policy Library dialog box.

3. Navigate through the policy library document to select a specific policy statement or group of statements, or click **Browse** and select a different library in which you can search for policy information.

   a. To navigate through the document, click a link related to the category or specific policy for addition.

   b. Click the copy icon after finding the category or statement for inclusion.

   c. Repeat steps a and b until you copy all of the appropriate categories and statements.

   Note
   You can search for words or phrases within a category or policy by typing the information in the **Search statements** field, and then clicking **Go**. If the first item that VPC displays is not the item you want, click **Next**.

4. Click **Close** after finishing your search, and then click **Save**.

To add text from a related document:

1. Launch the VPC Policy Editor.

2. Click **Related Document**.

   VPC displays the Related Policy Documents dialog box. This box contains all published policy documents.

3. Click the appropriate policy documents from the displayed list. To select more than one document, press **CTRL**, and then click to select non-consecutive policy documents. Press **SHIFT**, and then click to select consecutive documents.

4. Click **Submit**.

   VPC adds the selected policy documents to the open policy document.

5. Click **Save**.

To add a post note:

Like the preface note, you can add a post note to a document, category, subcategory, or statement using the item's editor. For example, you can add a post note to a category by clicking **Edit** to the right of the category name and clicking **Post Note**.

1. On the Edit page, click **Post Note**.

   VPC displays two new fields. You can add any type of information to these fields.

2. In the first field, type the subject information, such as a version number or effective date.

3. In the second field, type descriptive text, such as the document purpose.

Importing an XML Policy Document

You can import existing security policies that are in XML formats. VPC treats the imported policies like any other document, and you can use the VPC Policy Editor to view and edit the documents. The search function on the VPC User Site does not search the content of imported XML documents. However, when importing, you can associate “keywords” that display in a document search.

When you import an XML policy document, VPC automatically imports the document name and author, so you do not have to enter that information on the Import Document page.

To import an XML policy document:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Draft tab, click **Import**.
3. For **File Type**, click **XML**.
4. For **File**, type the file path and name or click **Browse** to select the file.
5. *Optional.* For **Version**, type a version number.
6. For **Policy Owner**, VPC references the user ID you used to log in to the Administration Site, and then automatically enters your user name in this field. If necessary, you can reassign the policy at any time to another person who “owns” or is responsible for this document.
7. *Optional.* For **Contributors**, type the names of the individuals who directly contributed to the content of the policy.
8. *Optional.* For **Approved By**, type the name of the person who approves this document before publishing the document to the User Site.
9. *Optional.* For **Key Words** field, type any words that relate to this document’s topic. Separate each word from the next with a comma (,). The VPC search engine uses the words entered in this field to locate this document when a user is performing a search.
10. *Optional.* For **Available From** and **Available To**, click a date range in which you want to offer this document to users once published.
11. Click **Import**.
12. On the Draft tab, select the policy and click **View** to verify that policy document imported correctly.

Editing the Content of a VPC Internal XML Policy Document

If you have the required permissions, you can modify the content of any policy document in Draft status. Use the following steps to edit a VPC XML document.

To edit a VPC internal XML policy document:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Draft tab, select the policy you want to edit and then click **Edit**.
3. Locate the section that you want to modify and edit the section as follows:
   - To remove the section, click **Delete** next to the section.
   - To modify the section, click **Edit** next to the section, type the edits, and then click **Save**.
   - To add a new section, next to **Add**, click the appropriate new section type, and then type the content in the newly created box.

4. When you complete your edits, click **View** and review your changes.
5. Click **Save**, and then click **OK** to save the changes.

Adding a URL to a VPC Internal XML Policy Document

You can add an image or URL link to a VPC XML document. VPC displays this information as an image or a link to an outside source. When adding an image, refer to the image using an absolute URL as shown in the following steps.

To add a URL to a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Draft tab, select the document for editing, and then click **Edit**.
3. Determine the placement for the URL within the document structure and then type the information in proper format, for example:

   ```
   <a href ="intranet/policy/PO.doc" target="_new"> PO policy </a>
   ```

4. Click **Save**.

Using the VPC Spell Checker

Once you enter the information necessary to create a document, review the spelling. The spell checker reviews the document for unknown words and suggests corrections. Use the following steps to run spell checker.

To check the spelling in a VPC Internal XML policy:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page with the Draft tab on top.

2. On the Draft tab, select the policy you want to edit and then click **Edit**.

   VPC displays the policy on the Edit page.

3. Click **Spell**.

   VPC displays the spell checker dialog box including each unknown word. The **Suggestions** list displays suggested spelling. You can stop spell checker at any time by clicking **Stop Checking**.

4. *Optional*. Type the correct spelling in the **Change to** field or click the correct word from the **Suggestions**.
5. *Optional*. Click **Ignore** for spell checker to continue checking and leave the unknown word. Use **Ignore All** for spell checker to ignore all instances of the unknown word.
6. *Optional*. Click **Change** when VPC displays the correct word in the **Change to** field. Use **Change All** for spell checker to change all instances of the unknown word.

   VPC displays the number of checked words.

7. Click **Submit**.
8. Click **Save**, and then click **OK** to save the changes.

Developing HTML Policy Documents

You use the VPC HTML Policy Editor to create and edit policy documents in HTML file format. The HTML Policy Editor provides a user-friendly format to help you quickly format text that you import, type, or paste into the editor. The HTML editor also supports easy insertion of tables, links, and graphics.

Note
Vector Markup Language (VML) is not supported in VPC. If you import an HTML document from Microsoft Office applications, you first must save the document as **Web Page, Filtered (*.htm, *.html)** before importing the document into VPC.

Creating an HTML Policy Document in VPC

The HTML Policy Editor uses TinyMCE to control editing. TinyMCE includes common features found in most word processors.

Note
By default, policy documents are available for one year from the creation date. You can change the document availability by adjusting the **Available From** and **Available To** dates in the Properties window for the document.

To create an HTML policy document in VPC:

1. On the Policy Center tab, click **New Policy**.

   VPC displays the New Policy page.

2. Click **Policy Editor**.

   VPC displays the Policy Editor page.

3. Click **HTML Policy Editor**, and then click **Submit**.

   VPC displays the HTML Editor page.

4. Type the document's title in the **Title** field and the author's name in the **Author** field.
5. Type or paste the appropriate text into the workspace under the toolbar.
6. Format the text.
   - To format paragraphs to look like policies created using the VPC Policy editor, click in the paragraph, and then select a section type from the **Styles** list.
   - To format paragraphs using typical HTML headings and body formatting, click in the paragraph, and then select a style from the **Format** list.
   - To override the default font in a paragraph, select the text, and then select a font from the **Font family** list.
   - To override the default font size, select the text, and then select a point size from the **Font size** list.
7. *Optional.* Use the toolbar buttons to continue formatting the text.
8. When you complete the document, click **Save** on the toolbar and then click **OK**.
9. Click **X** on the toolbar to close the editor. VPC closes the editor and places the new policy on the Draft tab of the View/Edit Policy page.

Importing an HTML Policy Document

You can import existing security policies in HTML format. VPC treats the imported policies like any other documents, and you can use the VPC HTML editor to view and edit the documents. The search function on the VPC User Site does not search the content of these imported documents. However, when importing, you can associate keywords that display in a document search.

Notes

- If the policy to import includes four or more images and image paths in the policy do not use HTTP protocol, zip the images directory before beginning this procedure so that you can import the images to the VPC server. When creating the zip file, clear the option to **Save full path info**. Otherwise, you have to manually update the finalized path to the images after importing the document.
- For detailed information and recommendations for working with graphics in HTML documents, see "Managing Images in HTML Policy Documents."

To import an HTML policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Draft tab, click **Import**.

   VPC displays the Import Document page.

3. For **File Type**, select **HTML**.
4. For **File**, type the path and the name of the file or click **Browse** to select the file.
5. *Optional.* If the document contains images that do not use HTTP protocol, select the images to import with the document.
   - If the document contains up to three images that do not use HTTP protocol, click **Browse** next to **Image 1** and select the first image file. Repeat to select **Image 2** and **Image 3** if the document has multiple images.
   - If the document contains four or more images that do not use HTTP protocol, click **Browse** next to **Zip File** and select the zip file containing the document images.
6. For **Title**, type the name of the policy document.
7. For **Author**, type the name of the person who wrote the policy.
8. *Optional.* For **Version**, type a version number.
9. For **Policy Owner**, VPC references the user ID you used to log in to the Administration Site, and then automatically enters your user name in this field. If necessary, you can reassign the policy at any time to another person who "owns" or is responsible for this document.
10. *Optional.* For **Contributors**, type the names of the individuals who directly contributed to the content of the policy.
11. *Optional.* For **Approved By**, type the name of the person who approves this document before publishing the document to the User Site.
12. *Optional.* For **Key Words** field, type any words that relate to this document's topic. Separate each word from the next with a comma (,).

    The VPC search engine uses the words entered in this field to locate this document when a user performs a search.

13. *Optional.* For **Available From** and **Available To**, click a date range in which you want to offer this document to users once published.

14. Click **Import**.

15. On the Draft tab, select the policy and click **View** to verify that the formatting, graphics, and links imported correctly.

Adding an Image to an HTML Policy Document

The HTML editor supports adding graphics to a policy document. You can link to a graphic through HTTP protocol or insert a graphic, in which case VPC uploads the graphic file to the VPC server. Use the following procedure to add an image to an HTML policy.

Note
For more information about using graphics with HTML documents, see "Managing Images in HTML Policy Documents."

To add an image to an HTML policy:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Draft tab, select the appropriate document, and then click **Edit**.

   VPC opens the policy in the HTML Editor.

3. In the document workspace area, click where you want to insert the image, and then click **Image/edit image**.

   VPC opens the Insert/edit image dialog box.

4. Specify the image file to insert by performing *one* of the following actions:

   - To link to an image stored on a server, for **Image URL**, type the full path and file name of the graphic you want to insert. For example, to include image `logo.gif` stored in the `Images` folder on the `pdxfs01` server, type `http://pdxfs01/Images/logo.gif`.
   - To insert a stored image file, click **or Upload Image** and type the full path and image name, or click **Browse** to locate the image.

5. *Optional.* For **Image description**, to assist visually impaired users, type a short description.

6. *Optional.* For **Image title**, if you want to name the image something other than the image description, type a name for the image.

7. *Optional.* For **Dimensions**, to lock the size of the image, type the width and height of the image in pixels. If you do not specify any dimensions, the editor may distort the image to fill the image field.

   Note
   To determine the dimensions of an image, open the image in a graphic editor, such as Microsoft Paint, and verify the attributes.

8. *Optional.* For **Border**, specify whether to include a border around the graphic. By default VPC includes a border. To remove the border, type `0`.

9. *Optional.* For **Alignment**, accept the default or select how to position the graphic in relation to the text around the graphic.

10. *Optional.* For **VSpace**, type the number of pixels of white space to include preceding and following the graphic.
11. *Optional.* For **HSpace**, type the number of pixels of white space to include to the left and right of the graphic.
12. *Optional.* To include images that display when a user moves the cursor over the inserted image, click **Alternative image**, and then for **mouse over** or **for mouse out**, type the full path and file name you want to include.
13. Click **Insert**.

    VPC closes the Insert/edit image dialog box and adds the graphic to the document.

14. On the HTML editor toolbar, click **Save**, and then click **OK**.

Inserting a Link in an HTML Policy Document

The HTML editor supports adding hyperlinks to any files that use HTTP protocol. For example, you can link to web pages, pictures, multimedia files, or documents stored on a network, internet, or the Intranet. Use the following steps to add a link to an HTML Policy.

To insert a link in an HTML policy:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Draft tab, select the appropriate document, and then click **Edit**.
3. Select either text or a graphic to use for the link and then click the link button on the editor toolbar.

   VPC opens the Insert/edit link dialog box.

4. For **Link URL**, type the full address to the destination file or web page using the format `http://<Web server>/<Path>/<File name>.` For example, to link to the NetIQ support page, type `http://www.netiq.com/support/default.asp`.
5. For **Title**, type the name of the destination page or file.
6. For **Target**, select where you want the destination file to show.
7. *Optional.* To include a second link in a popup dialog box, click **JS-Popup** and define the popup parameters.

   a. For **Popup URL**, type the full address to the destination file or web page using the format `http://<Web server>/<Path>/<File name>`.

   b. For **Window name**, type a name for the popup window.

   c. For **Size**, type the width and height of the popup window in pixels.

   d. For **Position (X/Y)**, type the coordinates to position the popup over the target window/frame. To position the popup in the center of the target window or frame, type `c / c`.

   e. Define the appearance of the popup window by selecting any of the **Show** options or **Make window resizable** option.

   f. Clear the **insert 'return false'** check box.

8. Click **Insert**.

   VPC closes the Insert/edit link dialog box and adds the link.

9. On the HTML editor toolbar, click **Save**, and then click **OK**.

Editing an HTML Policy

If you have the required permissions, you can modify the content of any policy document when the document is in Draft status. Use the following steps to edit an HTML policy document.

To edit an HTML policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page with the Draft tab on top.

2. On the Draft tab, select the policy you want to edit and then click **Edit**.

   VPC displays the policy in the HTML Editor.

3. Edit and format the text as appropriate.

   - For details about the toolbar buttons, click **?** on the HTML editor toolbar.
   - To format paragraphs to look like policies created using the VPC Policy editor, click in the paragraph, and then select a section type from the **Styles** list.
   - To format paragraphs using a typical HTML headings and body formatting, click in the paragraph, and then select a style from the **Paragraph** list.
   - To override the default font in a paragraph, select the text, and then select a font from the **Font** list.
   - To override the default font size, select the text, and then select a point size from the **Font size** list.

4. When you complete the document, click **Save** on the toolbar and then click **OK**.

5. Click **X** on the toolbar to close the editor. VPC closes the editor and places the new policy on the Draft tab of the View/Edit Policy page.

Developing Microsoft Word Policy Documents

Use the Word Policy Editor to create and edit policy documents in Microsoft Word (DOC or DOCX) format. The Word Editor includes the same formatting, editing, and reviewing features as Microsoft Word, so you can use the familiar toolbars and shortcuts to create and review text that you import, type, or paste into the editor. Like Microsoft Word, the Word Editor also supports easy insertion of tables, links, and graphics.

Note
To use the Word Editor, your computer must have a supported version of Microsoft Word and Internet Explorer with local intranet security settings set to download, run, and script safe ActiveX controls. For more information about requirements, see "Microsoft Word Document Requirements" on page 14.

Setting Your Browser to Use the Word Editor

The Word Editor requires a supported version of Internet Explorer with local intranet security settings set to download, run, and script safe ActiveX controls. Use the following procedure to modify your browser security settings to ensure you can use the Word Editor in VPC.

To set Internet Explorer to use the Word Editor:

1. On the **Start** menu, click **All Programs > Internet Explorer**.
2. On the **Tools** menu, click **Internet Options**.
3. On the Security tab, click **Local intranet** and then click **Custom Level**.
4. On the Security Settings dialog box, under **ActiveX controls and plug-ins**, select the permissions as shown in the following table:

Setting	Permission
Download signed ActiveX controls	Prompt
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe for scripting	Disable
Run ActiveX controls and plug-ins	Enable
Script ActiveX controls marked safe for scripting	Enable

5. Click **OK** to close the Security Settings dialog box, and click **OK** to close the Internet Options dialog box.

Using Toolbars in the Word Policy Editor

The Word Editor has two types of toolbars:

- The *VPC document toolbar* controls managing the document. This toolbar gives you options to open and save files, show or hide the Word toolbars, open the document properties dialog box, and close the editor.
- The *Word toolbars* are the same toolbars included in Microsoft Word. These toolbars allow you to work with the document content. The Standard and Formatting toolbars show by default.

To show or hide the Word toolbars, click **Hide/Show the toolbar** on the VPC document toolbar.

To display toolbars other than Standard and Formatting, right-click anywhere on the Word toolbar and select the toolbars that you want to display. The toolbars that you select remain until you hide the toolbars or close the editor.

Saving Documents in the Word Policy Editor

The document that displays in the Word Editor resides on the VPC server. VPC provides the following options for saving this current document:

- Save the current document to the VPC server
- Save a version of the current document to the VPC server
- Save the current document to your computer

Use one of the following procedures to save a Word document in the Word Editor.

To save the current document to the VPC server, click **Save the document** on the VPC Word Editor toolbar.

To save a version of the current document to the VPC server:

1. On the VPC Word Editor toolbar, click **Save as a new document**.

   VPC opens the Save As Options dialog box.

2. Click **Save a version at server**, and then click **OK**.

   VPC opens a version tracking dialog box.

3. *Optional*. Manage the existing versions of the document already stored on the VPC server.

   - To view an existing version, under **Existing Version**, click **Open**.
   - To remove an existing version, click **Delete**.
   - To see notes for a version, click **View Notes**.

4. Under **Notes for new version**, type a description of this version.

5. Click **Save New**.

To save the current document to your computer:

1. On the VPC Word Editor toolbar, click **Save as a new document**.

   VPC opens the Save As Options dialog box.

2. Click **Save on client machine**, and then click **OK**.

   VPC opens the Save As dialog box.

3. Enter a name for the document, and then click **Save**.

Creating a Microsoft Word Policy Document in VPC

Use the VPC Word Editor to create and edit policy documents in DOC or DOCX file format. The Word Policy Editor includes two types of toolbars:

- The *VPC Word Editor toolbar* controls managing the document. This toolbar gives you options to open and save files, show or hide the Microsoft Word toolbars, open the document properties dialog box, and close the editor.
- The *Microsoft Word toolbars* are the same toolbars included in Microsoft Word. These toolbars allow you to work with the document content. The Standard and Formatting toolbars show by default.

Note
To use the Word Editor, your computer must have a supported version of Microsoft Word and Internet Explorer with local intranet security settings set to download, run, and script safe ActiveX controls. For more information about requirements, see "Microsoft Word Document Requirements" on page 14.

To create a Microsoft Word policy document in VPC:

1. On the Policy Center tab, click **New Policy**.

   VPC displays the New Policy page.

2. Click **Policy Editor**.

VPC displays the Policy Editor page.

3. Click **Word Policy Editor**, and then click **Submit**.

   VPC displays the File Download dialog box to download the Word Editor Support Servlet, which supports the Word Policy Editor.

   Note
   To prevent the File Download dialog box from displaying each time you open the editor, clear **Always ask before opening this type of file**.

4. Click **Open**.
5. Type the document's title in the **Title** field.
6. *Optional*. To modify the default document properties, click **Edit Properties** on the VPC Word Editor toolbar. By default, VPC assigns the logged-on user as the document author and sets the document availability for one year from the creation date.
7. *Optional*. Display the Microsoft Word toolbars as appropriate:
   - ***To show or hide the Word toolbars,*** click **Hide/Show the toolbar** on the VPC document toolbar.
   - ***To display toolbars other than Standard and Formatting,*** right-click anywhere on the Microsoft Word toolbar and select the toolbars that you want to display. The toolbars that you select remain until you hide the toolbars or close the editor.
8. Type or paste the appropriate text into the workspace under the toolbars.
9. Format the text using the available toolbar buttons and commands.

   For more information about using the Microsoft Word tools, click **?** on the Standard Microsoft Word toolbar.

10. Save the document by clicking **Save the document** on the VPC Word Editor toolbar and VPC saves the document on the VPC Server.
11. Close the Word Editor by clicking **Cancel out of this screen** on the VPC Word Editor toolbar. VPC closes the Word Editor and adds the document to the Draft tab of the View/Edit Policy page.

Importing a Document in DOC/DOCX or RTF Format

You can import existing security policies in Microsoft Word DOC, DOCX, or RTF file format. VPC treats the imported documents like any other documents, and you can use the Word Editor in VPC to view and edit the documents.

The search function on the VPC User Site does not search the content of imported documents. However, when importing, you can associate "keywords" that display in a document search.

To import a DOC, DOCX, or RTF policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Draft tab, click **Import**.

   VPC displays the Import Document page.

3. For **File Type**, click the appropriate file type, **MS Word** or **Rich Text Format**.

4. For **File**, type the path and the name of the file or click **Browse** to select the file.

5. For **Title**, type the name of the policy document.

6. For **Author**, type the name of the person who wrote the policy.

7. *Optional.* For **Version**, type a version number.

8. For **Policy Owner**, VPC references the user ID you used to log in to the Administration Site, and then automatically enters your user name in this field. If necessary, you can reassign the policy at any time to another person who "owns" or is responsible for this document.

9. *Optional.* For **Contributors**, type the names of the individuals who directly contributed to the content of the policy.

10. *Optional.* For **Approved By**, type the name of the person who approves this document before publishing the document to the User Site.

11. *Optional.* For **Key Words** field, type any words that relate to this document's topic. Separate each word from the next with a comma (,).

    The VPC search engine uses the words entered in this field to locate this document when a user performs a search.

12. *Optional.* For **Available From** and **Available To**, click a date range in which you want to offer this document to users once published.

13. Click **Import**.

14. On the Draft tab, select the policy and click **View** to verify that policy document imported correctly.

Editing a Microsoft Word Policy Document

Provided you have the required permissions, you can modify the content of any policy document when the document is in Draft status. You use the VPC Word Editor to edit policy documents in Microsoft Word DOC or DOCX file format.

The Word Policy Editor includes two types of toolbars:

- The *VPC Word Editor toolbar* controls managing the document. This toolbar gives you options to open and save files, show or hide the Microsoft Word toolbars, open the document properties dialog box, and close the editor.
- The *Microsoft Word toolbars* are the same toolbars included in Microsoft Word. These toolbars allow you to work with the document content. The Standard and Formatting toolbars show by default.

Note
To use the Word Editor, your computer must have a supported version of Microsoft Word and Internet Explorer with local intranet security settings set to download, run, and script safe ActiveX controls. For more information about requirements, see "Microsoft Word Document Requirements" on page 14.

To edit a Microsoft Word policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page with the Draft tab on top.

2. On the Draft tab, select the policy you want to edit and then click **Edit**.

VPC displays the File Download dialog box to download the Word Editor Support Servlet, which supports the Word Policy Editor.

Note
To prevent the File Download dialog box from displaying each time you open the editor, clear **Always ask before opening this type of file**.

3. Click **Open**.

   VPC displays the Word Editor.

4. *Optional*. To modify the default document properties, click **Edit Properties** on the VPC Word Editor toolbar.

5. *Optional*. Display the Microsoft Word toolbars as appropriate:

   - ***To show or hide the Word toolbars,*** click **Hide/Show the toolbar** on the VPC document toolbar.
   - ***To display toolbars other than Standard and Formatting,*** right-click anywhere on the Microsoft Word toolbar and select the toolbars that you want to display. The toolbars that you select remain until you hide the toolbars or close the editor.

6. Edit and format the text as appropriate.

   For more information about using Microsoft Word tools, click **?** on the Standard Microsoft Word toolbar.

7. Save the document by clicking **Save the document** on the VPC Word Editor toolbar. VPC saves the document on the VPC Server.

8. Close the Word Editor by clicking **Cancel out of this screen** on the VPC Word Editor toolbar. VPC closes the Word Editor and adds the document to the Draft tab of the View/Edit Policy page.

Importing a Document in PDF or RTF Format

You can import existing security policies created in Adobe Acrobat (PDF) and Rich Text Format (RTF) formats. VPC treats these files like any other documents, with the following exceptions:

- VPC imports PDF and RTF documents as read-only. You cannot edit the files from within VigilEnt Policy Center.
- The search function on the VPC User Site does not search the content of the imported documents. However, when importing, you can associate keywords that display in a document search.
- PDF files require Adobe Acrobat or Adobe Reader to view the policy.

To import a PDF or RTF policy document:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Draft tab, click **Import**.
3. For **File Type**, click either **Acrobat PDF** or **Rich Text Format**.
4. For **File**, type the path and the name of the file or click **Browse** to select the file.
5. For **Title**, type the name of the policy document.
6. For **Author**, type the name of the person who wrote the policy.

7. *Optional.* For **Version**, type a version number.
8. For **Policy Owner**, VPC references the user ID you used to log in to the Administration Site, and then automatically enters your user name in this field. If necessary, you can reassign the policy at any time to another person who "owns" or is responsible for this document.
9. *Optional.* For **Contributors**, type the names of the individuals who directly contributed to the content of the policy.
10. *Optional.* For **Approved By**, type the name of the person who approves this document before publishing the document to the User Site.
11. *Optional.* For **Key Words** field, type any words that relate to this document's topic. Separate each word from the next with a comma (,).

    The VPC search engine uses the words entered in this field to locate this document when a user performs a search.
12. *Optional.* For **Available From** and **Available To**, click a date range in which you want to offer this document to users once published.
13. Click **Import**.
14. On the Draft tab, select the policy and click **View** to verify that policy document imported correctly.

Working with Document Templates and Samples

Document templates allow you to standardize policy document formats throughout your organization. They also speed up the creation process.

Creating a Policy Document Template

You can save any policy in the VPC database as a template. The template can then be accessed by click **New Policy > Templates**. Use the following steps to create a template.

To create a policy document template:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.
2. On the Draft tab, click the document to use as a template.
3. Click **Save**.

   VPC displays a verification message.
4. Click **OK** and VigilEnt Policy Center displays the selected file on the Template tab of the Policy Library.

Using a Template or Sample to Create a Policy Document

You can create a new policy document by copying an existing policy document and then editing it. The following procedure demonstrates using a template document from the Policy Library; however, you can use the same procedure to create a policy from a sample, a library policy, an archived policy, or any policy listed in the View/Edit Policy page.

Notes

- Only administrators and power users can copy all files types. Other users cannot copy a file of Microsoft Word, Adobe Acrobat PDF, or Rich Text Format type.
- You cannot copy imported Adobe Acrobat PDF or Rich Text Format (RTF) documents.
- To change a document that you cannot copy, export the document, make the edits, and then import the document.

To create a policy document using an existing document:

1. On the Policy Center tab, click **New Policy**.

   VPC displays the New Policy page.
2. Click **Policy Samples**.

   VPC displays the Policy Library page with the Sample tab on top.
3. Click the tab containing the appropriate policy: Sample, Template, Library, or Archived.
4. Select the policy you want to use to create the new policy, and then click **Copy**.

   VPC displays a verification message.
5. Click **OK**. VPC adds the copy to the Draft tab of the View/Edit Policy page.

To change the sample policy document:

1. On the Draft tab of the View/Edit Policy page, select the copy of the policy sample and click **Edit**.

   VPC displays the Edit page.
2. Make changes, such as changing the policy name and author.

   Note

   You can move categories up one place at a time when editing a document. Click the move button adjacent to the category that you want to move. VPC moves the category up one place. Click again to move up another place.
3. Click **Save**.

   VPC displays a verification message.
4. Click **OK**.

Chapter 8
Managing Policy Documents

VPC provides a variety of tools and features to help you manage policy documents once you have created or imported the documents. VPC grants manage (**M**) and read not required (**NR**) privileges to document owners by default when the user creates a document.

Working with Policy Documents

Document managers may want to modify policy documents in VPC. Depending on the permissions of the document manager, they can perform a variety of tasks. This section describes several of those tasks.

Viewing a Policy Document

You can view a policy document in any stage of its life-cycle. The steps are the same when viewing a document from any of the **View/Edit Policy** and **Policy Library** lists. Perform the following steps to view a policy document.

To view a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.
2. Select the document for viewing, and then click **View**.

   Note
   The document properties no longer open in a separate window when you view the policy. To access the properties, navigate to the View/Edit Policy page, select the document for viewing, and then click **Properties**.

3. Scroll through the policy document to view its contents.
4. Click **Close** to return to the View/Edit Policy page after viewing the document.

Printing a Policy Document

The procedure to print a policy document depends on the document file type. Use one of the following procedures to print a policy document.

Note
For more information about document file types, see “Understanding Document File Types.”

To print an internal (XML) policy document:

1. From the View/Edit Policy page, select the XML file that you want to view, and then click **View**.

   VPC displays the item in the Document Viewer window.

2. Click **Print**.

   VPC displays the Print dialog box.

3. Select your printing preferences, and then click **OK**.

To print a Microsoft Word policy document:

1. From the View/Edit Policy page, select the DOC or DOCX file that you want to view, and then click **View**.

   VPC displays the item in the Microsoft Word-enhanced window.

2. Click **Print** on the Microsoft toolbar.

To print an HTML policy document:

1. From the View/Edit Policy page, select the HTML file that you want to view, and then click **View**.

   VPC displays the item in the Document Viewer window.

2. Right-click inside the Document Viewer window and select **Print**.

   VPC displays the Print dialog box.

3. Select your printing preferences, and then click **OK**.

To print a PDF policy document:

1. From the View/Edit Policy page, select the PDF file that you want to view, and then click **View**.

   VPC displays the item in the Adobe-enhanced window.

2. Click **Print** on the Adobe toolbar.

   VPC displays the Print dialog box.

3. Select your printing preferences, and then click **OK**.

Searching For a Policy Document

If your policy document is in the VPC internal format, you can search for specific text by using the VPC Policy Editor. The editor filters documents based on text, audience, and environment, or any combination.

Note

For more information about document file types, see “Understanding Document File Types.”

To search for policy documents:

1. Log on to the Administration Site.

2. Click **Search**.

   VPC displays the Search Policies dialog box.

3. Type the word or phrase for which you want to search.

4. Specify the **Scope** of your search.
   - Select **All** to search all titles, keywords, and custom properties of policy documents. The **All** option also includes a full text search of policy documents that are in HTML or XML format.
   - Select **Title/Keywords** to search only the titles and keywords of policy documents.
   - Select **Custom Properties** to search only the custom properties assigned to policy documents.
5. Click **Go**.

   VPC displays an update message until it finds and displays the matching files.
6. Use the results to locate the policy document you want. If you click the document name, VPC opens the policy in the current window. You can also click the folder name link to open the folder and view all policies in that folder.
7. ***If you want to print the list of policy documents found in the search***, click **Print**.
8. ***If you want to export the list of policy documents to a file***, click **Export**.

Searching for Text in a Policy Document

VPC provides a search for specific text by using the Policy Editor and filters documents based on text, audience, and environment, or any combination.

To search documents by a statement:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Draft tab, select a policy document, and then click **Edit**.
3. On the Edit page, click **Category**, and then click **From Library**.
4. On the Policy Library page, type the statement text in the Search statements field, and then click **Go**. VigilEnt Policy Center searches through all of the source documents in the Policy Library and displays the first reference detected. ***If the first item that VPC displays is not the item you want,*** click **Next**.

Managing Default Policy Document Properties

Document properties such as the version, approved by, and available date reside in the document properties area. Use the following steps to manage the detail within each policy document.

Note

You may receive an error if you click **Cancel** while in the Policy Property Editor window. If this error occurs, resolve the error by following the steps in "Increasing Your Temporary Internet Disk Space" on page 142.

To manage default policy document properties:

1. On the Policy Center tab, click **View/Edit Policy**.
2. Click the appropriate policy document, and then click **Properties**.
3. Make any necessary changes, and then click **Save**.

Linking a Policy Document to an Item

You can link a policy document or quiz to another file such as a news item or email message. This feature is particularly useful when you want to alert users to a new document by adding the link to the notification email message. That way they can click the link to open the document rather than first accessing the User Site and looking for the new document. You can link to policy documents or quizzes in the Review and Published phases. Use the following steps to link a policy document to an item.

Note
For information about linking a quiz to an item, see "Linking a Quiz to an Item."

To link a policy document to an item:

1. On the Policy Center tab, click **View/Edit Policy**.
2. Select the document you want to add to an item, and then click the Properties button.

   The URL address to copy into the item resides at the bottom of the page in the **User Site Access Links** section.
3. Copy the URL.
4. Paste the text of the URL where you want the link, such as the content of an email message.
5. Verify the URL string ensuring the protocol, server name, and port are correct for linking to the User Site.

   Note
   For more information about linking a quiz to an item, see "Linking a Quiz to an Item" on page 114.
6. ***If you want the linked document to open in its own window***, paste the link information in the following format:

   ```
   <a href="http://servername:8080/policy/launch.jsp?cmd=X-X-X-X-X"
   target="_blank">
   ```
   Where `http:// servername:8080/policy/launch.jsp?cmd= X-X-X-X-X` is the URL copied from the Properties page displaying the links for the policy documents.
7. In the Properties window, click **Cancel** to return to the View/Edit Policy page.

Reassigning a Policy Document

The VigilEnt Policy Center administrator can assign a document from one user to another. This feature is necessary if a user leaves your company and the replacement cannot access that user's files. By reassigning the documents, another user can access and maintain those documents. Use the following steps to reassign a document.

To reassign a document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.
2. Select the policy document that you want to reassign, and then click **Reassign**.
3. In the **Role** field, select the role of the user account to which you want to reassign the policy document.

4. In the **Search for Users** field, type the name of the user account to which you want to reassign the policy document, and then click **Search**. You can search for all users by clicking **Search** without making an entry in the **Search for Users** field.

5. Click the appropriate user from the displayed list.

6. Click **Submit** and VPC assigns the policy document to the new owner.

Applying User Access to a Policy Document

When you create a new document, by default VPC applies the Everyone – Read ACL. You can modify the access permissions for a document by applying an existing ACL or by creating a new ACL for the document.

Notes

- For more information about ACLs, see "Understanding Access Control Lists (ACLs)."
- To require administrators to apply ACLs to all review or published documents, see "Setting ACL Automation."

Applying an Existing ACL to a Policy Document

If your organization has a set of preconfigured ACLs, you can modify the access permissions for a document by applying one of the existing ACLs to the policy document. Use this procedure to apply an existing ACL to a policy document.

Notes

- For more information about ACLs, see "Understanding Access Control Lists (ACLs)."
- To require administrators to apply ACLs to all review or published documents, see "Setting ACL Automation."

To apply an existing ACL to a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

2. On the Draft, Review, or Published tab, select the appropriate document and click **ACL**.

3. Click the **By ACL** tab.

4. Under **Available ACLs**, select the appropriate ACL(s) and click **>>** to move the ACLs to the **Selected ACLs** box.

5. Click **Save**.

Applying User Permissions Directly to a Policy Document

You can modify the access permissions for a document by creating a new ACL for the document. This procedure creates a hidden ACL that is specific to the document. Use this procedure to create a new ACL for a policy document.

Notes

- To create a reusable ACL, first use the ACL editor to create a new ACL (see “Creating an Access Control List”), and then use the By ACL tab to apply the ACL.
- To require administrators to apply ACLs to all review or published documents, see “Setting ACL Automation.
- For more information about ACLs, see “Understanding Access Control Lists (ACLs).”

To apply users directly to a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Draft, Review, or Published tab, select the appropriate document and click **ACL**.

   The Manage Access Control for a Document window opens.

3. Click the By User tab.
4. Under **Set the access privileges**, select one or more of the access permissions:
   - **Required to Read (RR)**: Requires users to acknowledge that they have read a specific document.
   - **Read but Not Required (NR)**: Permits users to read a published document, but does not require proof that the reader read the document. Use this option if you want a public domain document available for users to read, but does not require that your users read the document.
   - **Review (RV)**: Permits users to review a document in the Review phase.
   - **Manage (M)**: Permits power users to make changes to the content of a document.

   Note

   If you have multiple power users who may edit a specific document, assign the **Manage** privilege to each user or VPC allows edits by only one user. Assign the **Manage** privilege to only power users who have access to the Administration Site.

5. Search for the users or groups to associate with the access permissions selected in step 4. In the box next to **Search**, type the search criteria. VPC accepts wildcard characters such as asterisks (*).
   - To limit the search to only groups, click **Groups only search**.
   - To search for groups and users, click **Include groups in search**.
6. Click **Search** to populate the **Available Users/Groups** box with the search results.
7. Select the users or groups that you want to have access to the document, and then click **>>** to move them to the **Selected Users/Groups** box.
8. Click **Save**.

Adding Language Equivalent Policy Documents

You can add language equivalent copies of policies to a master policy enabling users to view the master policy content in their native language. Any number of language equivalent copies can be associated with a master version of a policy without affecting policy workflow or reporting.

Note
Master policies are policies that are created or imported into the site by policy creators. State changes, policy ownership, ACL associations, and compliance reporting data retain their direct correlation to the master policy. Language equivalent copies of the master policy are accessible only to those users that have proper access privileges for viewing the master.

To add a language equivalent copy to a policy:

1. On the Policy Center tab, click **View/Edit Policy**.
2. Select the policy for viewing, and then click **Properties**.
3. On the Properties page, click the Languages tab.
4. Enter the translated title for the targeted language.

   Note
   For more information about managing the languages for which policy equivalents are to be uploaded, see "Setting Language Preferences" on page 72.

5. Browse to upload the associated file, and select the appropriate file type and language from the available options.

   Note
   HTML, Microsoft Word, and PDF documents are the only supported language equivalent formats. VPC does not translate the uploaded documents but offers a means to display the translated copies of existing policies.

6. Click **Add** to upload the new language equivalent copy of the policy.
7. ***If you want to view and delete language equivalent copies of policies***, select the document and click the appropriate icon.
8. Click **Close** to close the window.

When language equivalent copies of policy are added to master policies, the following occurs on the User Site with regard to how users will interact with the translated items:

- VPC displays translated titles and policies automatically when the User Site language interface designation matches language availability for a policy and its title. If the interface language is set to Spanish and a master policy has an associated Spanish equivalent policy and title, then the translated versions of each display on the User Site.
- VPC displays the primary language version of a policy when (a) the desired language for a policy is not available for viewing, or (b) when the title has been translated but no language equivalent copy of the policy has been uploaded to the site.
- In the User Site document viewer, if a policy exists in multiple language formats a language selection menu is visible in the lower-left corner of the title pane. Users can select from the available languages for viewing the copies of the policy.

Note
The languages offered for User Site interface text are limited to a set of seven languages. However, the ability to display policy language equivalents comprises a broader language set and is more flexible to meet the demands of native language policy requirements. While the interface text is not yet available in Thai, the ability to upload a translated Thai policy will greatly enhance an organization's ability to address the language needs of their users.

Reviewing Policy Documents

Because policy documents are vital to an organization’s success, verify that the documents are current and correct. You can verify content by sending a policy through a review process before publishing the document to the User Site.

Submitting a Policy Document for Review

Because policy documents are vital to an organization’s success, verify that the documents are current and correct. You can verify content by sending a policy through a review process before publishing the document to the User Site. Use the following steps to submit a policy document for review.

Note
Apply **Review** ACLs to a policy document before submitting the document for review. For more information, see “Applying User Access to a Policy Document.”

To submit a policy document for review:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Draft tab, select the document to submit for review, and then click **Review**.

   VPC displays a verification message.

3. Click **OK** and VPC displays the document on the Review tab.

Viewing Comments on a Policy Document

You can set up policy documents for users to submit comments on the selected file. Use the following steps to view comments made by users on a policy document.

To view comments on a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Review tab, select the policy document for viewing, and then click **Comments** and VPC displays the comments for the selected policy document.

Rejecting a Policy Document

A document owner can either accept and publish a policy document on the Review tab, or reject to document back to the Draft tab. If you reject a policy document, VPC moves the document from the Review tab to the Draft tab. You may re-send a rejected document for review. Use the following steps to reject a policy document.

To reject a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.

2. On the Review tab, select the document for rejection, and then click **Reject**.

   VPC displays a verification message.

3. Click **OK** and VPC displays the policy document on the Draft tab.

Publishing Policy Documents

Once a policy document receives approval on the Administration Site, the administrator can publish the document to the User Site for reading by all employees with access to the company intranet.

Publishing a Policy Document

Once a policy document receives approval on the Administration Site, the administrator can publish the document to the User Site for reading by all employees with access to the company intranet. Use the following steps to publish a policy document.

To publish a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

2. On the Review tab, select the document to publish, and then click **Publish**.

3. Click **OK** and VPC displays the policy document on the Published tab and on each user’s Home page in the User Site.

Validating a Published Document

By running a log report for a published document, you can verify that the file has not been corrupted or changed by someone other than the author. Use the following steps to validate a published document.

To validate a published document:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the Published tab, select the document to validate, and then click **Log**.

   VPC displays a message window indicating whether the file matches the original file.
3. Click **OK**.

Sending a Policy Document Notification

VigilEnt Policy Center automates the task of notifying people when you submit a document for review or publish the document. The email feature creates an email message that includes a link to the document and populates the recipient field with those users and groups who can access the document. Before sending the message, you can customize the message to your requirements. Use the following procedure to send an email notification for a document.

Notes

- VPC requires you to configure mail server information before you can use the VPC email feature. For more information, see “Configuring VPC to Use a Mail Server.”
- To require email notifications for all or published documents, use the **Automate E-mail Notification** options when configuring mail server information.

To send a document notification:

1. On the Policy Center tab, click **View/Edit Policy**.
2. On the appropriate tab, select the appropriate document and click **E-mail**.
3. *Optional*. Modify the **From**, **To**, **Subject**, **Cc**, and **Bcc** fields as appropriate.
4. For **Message Text**, in the URL located in the third paragraph, replace `localhost` with the name of the server hosting VPC.

   Note
   The email message includes the URL as an active hyperlink.
5. Delete the first paragraph of the message text, and modify the message.
6. Click **Submit** to send the notification.

   VPC displays a confirmation that the email was sent successfully.
7. Click **Close** to return to the View/Edit Policy page.

Organizing and Storing Policy Documents

VPC supports setting folders to store similar policy documents and quizzes. For example, you can create a folder named "Email Documents" and include an email policy and the related quiz. VPC also supports archiving documents, which removes the documents from view in the User Site but saves the documents for reference and future use.

Note

NetIQ Corporation recommends developing a folder structure and naming scheme before you begin importing and creating documents. For more information, see "Organizing Documents."

Adding a Policy Document to a Folder

Once you set up your folders, you can add policies and quizzes in the draft, review, or published phase. You cannot add an archived document to a folder because VPC stores the document in the folder where the document resides at the time of the archiving action. Use the following steps to add a policy document to a folder.

Notes

- For information about creating folders, see "Creating Folders."
- If you are updating VPC from a previous version, VPC assigns to the root folder all policy documents previously not assigned to a folder.

To add a policy document to a folder:

1. On the Policy Center tab, click **View/Edit Policy**.
2. Click the appropriate document, and then click **Add To**.
3. Click **Add Documents** under the appropriate folder, and then click **Save**.

   VPC adds the document to the folder.
4. Click **Close** to return to the View/Edit.

Exporting a Policy Document

You can export documents from VigilEnt Policy Center into XML or HTML format files and store or archive the data outside of VPC. Use the following steps to export a policy document.

To export a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.
2. On the Draft, Review, Published, or Archived tab, select the policy document for exporting, and then click **Export**.

   VPC displays the Export Document page.
3. Select the appropriate **File Type**.

4. ***If you want to include information about the document, such as the author's name, when exporting an HTML file,*** click **Yes** next to **Include signature line for HTML files**.
5. Click **Export**, and then follow the steps in the wizard to export the document.

Archiving a Policy Document

Archiving a policy document removes the document from view in the User Site and saves the document for reference and future use. To save time when creating a new policy document similar to an archived document, you can copy the archived policy document and make the necessary changes to create a new document. Use the following steps to archive a policy document.

To archive a policy document:

1. On the Policy Center tab, click **View/Edit Policy**.

   VPC displays the View/Edit Policy page.
2. On the Published tab, select the policy document for archiving, and then click **Archive**.

   VPC displays a verification message.
3. Click **OK** and VPC displays the selected policy document on the Archived tab and the removes the document from the User Site.

Archiving a Policy Library

An administrator can remove a policy library from view on the Library tab by using the archiving feature. Archiving saves the library for later reference, but you cannot access the library from the Library tab. Use this function when you want to use a new library and keep the older library available for legal reference. Use the following steps to archive a policy library.

To archive a policy library:

1. On the Policy Center tab, click **Policy Library**.

   VPC displays the Policy Library page.
2. On the Library tab, select the policy library that you want to archive, and then click **Archive**.

   VPC displays a verification message.
3. Click **OK** and VPC moves the selected policy library to the Archived tab.

Chapter 9
Creating and Managing Quizzes

This chapter includes information about creating, maintaining, and deploying quizzes. Be sure to review the multiple ways you can create a quiz, whether you import an existing quiz, create a quiz using some material offered in VPC, or copy an available quiz.

Creating Quizzes

Quizzing users is a true test of their knowledge of policy documents. You can create a quiz by copying a sample quiz or by updating an archived quiz.

Creating a Quiz Using the Quiz Editor

You can create a new quiz using the Quiz Editor in VPC. By requiring your users to meet a minimum grade, you can verify that your users read and comprehend your policy documents. Use the following steps to create a new quiz using the Quiz Editor.

To create a quiz using the quiz editor:

1. On the Education tab, click **New Quiz**, and then click **Quiz Editor**.
2. Type a **Title** and **Author**.
3. *Optional.* Type a description of the quiz in the **Description** field.
4. *Optional.* Type a **Version**, **Quiz Owner**, and **Approved By**.
5. *Optional.* Type search information in the **Key Words** field.
6. Verify the **Available From** and **Available To** dates.
7. Type a **Passing Grade**.
8. ***If you want to add a logo graphic to this quiz,*** complete the following steps:
   a. Include the path and file name of the graphic in the **Logo Image** field. To ensure that path and file name are correct, click **Browse** to navigate to the file location.
   b. View the logo before saving your changes by click **Set**. You can also delete the logo by clicking **Remove**.
9. Click **Save**.

   VPC displays a verification message.
10. Click **OK**, scroll down, and then click **Add**.

VPC displays the Quiz Editor page.

11. In the **Order Index** field of the Questions dialog box, type the numerical place within the quiz where you want this question to display. The questions on the quiz display in order beginning with 1.
12. In the **Question Weight** field, type the weight of the question compared to the other questions in the quiz.
13. To include this question in the quiz, click **Make Question Available**. Clear this field to retain the question and prevent the quiz from displaying the information.
14. In the **Question Text** field, type the text for the question.

Note
If you cut and paste information from Microsoft Word into the Question Text field, manually replace any apostrophes (‘) or quotes (“).

15. ***If you want to use a graphic in the question,*** complete the following steps:
    a. Include the path and file name of the graphic in the **Image** field. To ensure that path and file name are correct, click **Browse** to navigate to the file location.
    b. View the graphic before saving your changes by clicking **Set**. You can also delete the graphic by clicking **Remove**.
    c. Select the appropriate layout setting. For example, to display the graphic before the question text, click **Image followed by text**.
16. In the Answer dialog box, type an answer to the question in the **Answer Text** field.
17. In the **Answer Weight** field, type the weight of this answer compared to the other answers for this question.
18. ***If you want to use a graphic in the answer,*** complete the following steps:
    a. Include the path and file name of the graphic in the **Image** field. To ensure that the path and file name are correct, click **Browse** to navigate to the file location.
    b. Select the appropriate layout setting. For example, to display only the graphic as the answer, click **Image only**.
19. Click **Add Answer**.
20. Repeat Step 16 through Step 19 for each answer to the question.
21. Type the correct answer in the **Feedback** field and include an explanation.

Note
You can add information to the **Feedback** field to explain the correct answer to a specific question. For example, you can include a current event in the Feedback field to help illustrate the timeliness of the associated question. VPC includes this information when exporting a document to XML format.

22. View the answers before submitting the changes by clicking **Preview**.
23. Click **Submit**, and then click **Save**.

Creating a Quiz Using a Sample

VPC provides sample quizzes to save time when creating quizzes. You can create a new quiz from a sample, and then make any necessary changes. For information about making changes, see “Editing Quizzes.” Use the following steps to create a new quiz by copying a sample quiz.

To create a quiz using a sample:

1. On the Education tab, click **New Quiz**, and then click **Quiz Samples**.
2. Select the “E-mail Security - Sample Quiz,” and then click **Copy**.
3. Click **OK**.

Importing a Quiz

Your organization already may have some documents existing in an XML format. You can import these files into VPC and establish a quiz for your users. Use the following steps to import an XML file.

To import a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. On the Draft tab, click **Import**.

   VPC displays the Import Quiz page.

3. Type the name of the file in the **File Name** field or click **Browse** to select the file.
4. Click **OK**.

Editing Quizzes

VPC offers several options to modify a quiz in the VPC database.

Changing Quiz Information

By using the Edit function, you can change a quiz name, author, and availability dates. You can also add, delete, and hide quiz questions. Use one or more of the following procedures to change a quiz.

To change the quiz information:

1. On the Education tab, click **View/Edit Quiz**.
2. Click the quiz that you want to edit, and then click **Edit**.
3. Make any changes, and then click **Save**.

To add a quiz question:

1. On the Education tab, click **View/Edit Quiz**.
2. Click the quiz for editing, and then click **Edit**.
3. Under **Questions**, click the first **Add** button.

4. In the **Order Index** field of the Questions dialog box, type the numerical place within the quiz where you want this question to display. The questions on the quiz display in order beginning with 1.

5. In the **Question Weight** field, type the weight of the question compared to the other questions in the quiz.

6. To include this question in the quiz, click **Make Question Available**. Clear this field to retain the question and prevent the quiz from displaying the information.

7. In the **Question Text** field, type the text for the question.

Note
If you cut and paste information from Microsoft Word into the Question Text field, manually replace any apostrophes (‘) or quotes (“).

8. ***If you want to use a graphic in the question,*** complete the following steps:

    a. Include the path and file name of the graphic in the **Image** field. To ensure that path and file name are correct, click **Browse** to navigate to the file location.

    b. View the graphic before saving your changes by clicking **Set**. You can also delete the graphic by clicking **Remove**.

    c. Select the appropriate layout setting. For example, to display the graphic before the question text, click **Image followed by text**.

9. Under **Answers**, type an answer to the question in the **Answer Text** field.

10. In the **Answer Weight** field, type the weight of this answer compared to the other answers for this question. For example, if you enter the correct answer, type `100`. If you enter a partially correct answer, you may want to type `50`.

11. ***If you want to use a graphic in the answer,*** complete the following steps:

    a. Include the path and file name of the graphic in the **Image** field. To ensure that the path and file name are correct, click **Browse** to navigate to the file location.

    b. Select the appropriate layout setting. For example, to display only the graphic as the answer, click **Image only**.

12. Click **Add Answer**.

13. Repeat Step 9 through Step 12 for each answer to the question.

14. Type the correct answer in the **Feedback** field and include an explanation.

Note
You can add information to the **Feedback** field to explain the correct answer to a specific question. For example, you can include a current event in the Feedback field to help illustrate the timeliness of the associated question. VPC includes this information when exporting a document to XML format.

15. View the answers before submitting the changes by clicking **Preview**.

16. Click **Submit**, and then click **Save**.

To add a quiz question from the library:

1. On the Education tab, click **View/Edit Quiz**.

2. Click the quiz for editing, and then click **Edit**.

3. Under **Questions**, click the second **Add** button to add a question from the library.

4. Find the appropriate question, and then click the add question button next to the question.
5. Click **Close** when you are finished.

   VPC adds the question and all of its associated information, such as answer and question weight, to the quiz.
6. Click **Save**, and then click **OK**.

To delete a quiz question:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.
2. Click the quiz for editing, and then click **Edit**.

   VPC displays the Quiz Editor page.
3. Click a question, and then click **Delete**.

   VPC displays a verification message.
4. Click **OK**. VPC removes the questions from the Questions dialog box, renumbers the questions, and saves the changes.

To hide a quiz question:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.
2. Click the quiz for editing, and then click **Edit**.

   VPC displays the Quiz Editor page.
3. Click a question, and then click **Hide/Show**.
4. Click **OK**. The question remains in the quiz, but VPC does not display the question.

Managing Quiz Properties

Quiz properties such as the version, approved by, and available date range reside in the document properties area.

To manage default quiz properties:

1. On the Education tab, click **View/Edit Quiz**.
2. Select the appropriate quiz, and then click **Properties**.

   VPC displays the Properties dialog box.
3. Make any necessary changes, and then click **Save** and VPC saves your changes.

Adding HTML to a Quiz

VPC accepts an image or URL link on a quiz. VPC displays the information as an image or a link to an outside source. When adding an image, refer to the image using an absolute URL. Use these steps to add HTML to a quiz.

To add a URL to a quiz:

1. On the Education tab, click **View/Edit Quiz**.
2. On the Draft tab, click the quiz for editing, and then click **Edit**.

   VPC displays the Quiz Editor page.
3. Click the appropriate question, and then click **Edit**.

   VPC displays the Question dialog box.
4. Locate within the text box where to add the URL, and then type the information in proper format, for example:

   ```
   <a href =“intranet/policy/travel.doc” target=“_new”> travel policy </a>
   ```
5. Click **Submit**.

Linking a Quiz to an Item

Linking lets you link a policy document or quiz to another file such as a news item or email message. This feature is particularly useful when you want to alert users to a new quiz by adding the link to the notification email message. Then users can open the quiz by clicking the link rather than first accessing the User Site and looking for the new quiz. You can link to quizzes in the Review or Published phase. Use the following steps to link a quiz to an item.

Note

For information about linking a policy document to an item, see “Linking a Policy Document to an Item.

To link a quiz to an item:

1. On the Education tab, click **View/Edit Quiz**.
2. Select the quiz that you want to add to an item, and then click the Properties button.

   The URL address to copy into the item resides at the bottom of the page in the **User Site Access Links** section.
3. Copy the URL.
4. Paste the text of the URL where you want the link, such as the content of an email message.
5. Verify the URL string ensuring that the protocol, server name, and port are correct for linking to the User Site.

   Note

   For more information about linking a policy document to an item, see “Linking a Policy Document to an Item” on page 100.
6. ***If you want the linked quiz to open in its own window***, paste the link information in the following format:

   ```
   <a href="http://servername:8080/policy/launch.jsp?cmd=X-X-X-X-X"
   target="_blank">
   ```

   Where `http:// servername:8080/policy/launch.jsp?cmd= X-X-X-X-X` is the URL copied from the Properties page displaying the links for the quiz.
7. In the Properties window, click **Cancel** to return to the View/Edit Quiz page.

Reassigning a Quiz

The VigilEnt Policy Center administrator can assign a quiz from one user to another. Use this feature when a user leaves your company and the replacement cannot access that user's files. By reassigning your quizzes, another user can access and maintain those quizzes. Use the following steps to reassign a quiz.

To reassign a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. Select the quiz that you want to reassign, and then click **Reassign**.
3. In the **Role** field, select the role of the user account to which you want to reassign the quiz.
4. In the **Search for Users** field, type the name of the user account to which you want to reassign the quiz, and then click **Search**. You can search for all users by clicking **Search** without making an entry in the **Search for Users** field.
5. Click the appropriate user from the displayed list.
6. Click **Submit** and VPC assigns the quiz to the new owner.

Setting Access Permissions for a Quiz

When you create a new document, by default VPC applies the Everyone – Read ACL. You can modify the access permissions for a quiz by applying an existing ACL or by creating a new ACL for the document. Use one of the following procedures to set access permissions for a document.

Notes

- For more information about ACLs, see "Understanding Access Control Lists (ACLs)."
- To require administrators to apply ACLs to all review or published documents, see "Setting ACL Automation."

To apply an existing ACL to a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. On the Draft, Review, or Published tab, select the appropriate document and click **ACL**.

   The Manage Access Control for a Document window opens.

3. Click the **By ACL** tab.
4. Under **Available ACLs**, select the appropriate ACL(s) and click **>>** to move the ACLs to the **Selected ACLs** box.
5. Click **Save**.

To apply users directly to a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. On the Draft, Review, or Published tab, select the appropriate document and click **ACL**.

   The Manage Access Control for a Document window opens.

3. Click the By User tab.

Notes

- Using the By User tab to apply users to a document creates a hidden ACL specific to this document.
- To create a reusable ACL, first use the ACL editor to create a new ACL, and then use the By ACL tab to apply the ACL.

4. Under **Set the access privileges**, use the following permissions:
   - **Required to Read (RR)**: Requires users to acknowledge that they have read a specific document.
   - **Read but Not Required (NR)**: Permits users to read a published document, but does not require proof that the reader read the document. Use this option if you want a public domain document available for users to read, but does not require acknowledgement.
   - **Review (RV)**: Permits users to review a document in the Review phase.
   - **Manage (M)**: Permits users to make changes to document content.

   Note

   If you have multiple power users who may edit a specific document, assign the **Manage** privilege to each user or VPC allows edits by only one user.

5. Search for the users and groups to associate with the access permissions selected in step 4. In the field next to **Search**, type the search criteria. VPC accepts wildcard characters such as asterisks (*).
   - To limit the search to only groups, click **Groups only search**.
   - To search for groups and users, click **Include groups in search**.
6. Click **Search** to populate the **Available Users/Groups** box.
7. Select the users or groups that you want to have access to the document, click **>>** to move them to the **Selected Users/Groups** box, and then click **Save**.

Reviewing and Publishing Quizzes

To ensure accurate quiz content and test users on all aspects of a policy, document administrators send quizzes through a review process before publishing them to the User Site.

Submitting a Quiz for Review

Accurate and thorough quizzes test users on all aspects of a policy document. Verify content by sending a quiz through a review process before publishing to the User Site. The following steps provide information about submitting a quiz for review.

Note

Before submitting a quiz for review, apply Review ACLs to the quiz. For more information, see “Setting Access Permissions for a Quiz.”

To submit a quiz for review:

1. On the Education tab, click **View/Edit Quiz**.
2. On the Draft tab, select the quiz to submit for review, and then click **Review**.
3. Click **OK**.

Viewing Comments on a Quiz

You can set up quizzes for users to submit comments on the selected file. Use the following steps to view comments made by users on a quiz.

To view comments on a quiz:

1. On the Education tab, click **View/Edit Quiz**.
2. On the Review tab, select the quiz for viewing, and then click **Comments**. VPC displays the comments for the selected quiz.

Rejecting a Quiz

Quiz administrators send quizzes for review before publishing to verify accuracy. A reviewer may reject a quiz for any reason. If you reject a quiz, VPC moves the quiz from the Review tab to the Draft tab. The following steps show you how to reject a quiz.

To reject a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.
2. On the Review tab, select the quiz for rejection, and then click **Reject**.

   VPC displays a verification message.
3. Click **OK**.

Publishing a Quiz

An owner can publish a quiz at any time. A published quiz posts to the User Site, making the quiz available to users assigned required to complete the quiz. Use the following steps to publish a quiz to the User Site.

To publish a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.
2. On the Review tab, select the quiz for publication, and then click **Publish**.

   VPC displays a verification message.
3. Click **OK**.

Validating a Published Quiz

By running a log report for a published quiz, you can verify that the file has not been corrupted or changed by someone other than the author. Use the following steps to validate a published quiz.

To validate a published quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. On the Published tab, select the quiz to validate, and then click **Log**.

   VPC displays a message window indicating whether the file matches the original file.

3. Click **OK**.

Sending a Quiz Notification

VigilEnt Policy Center automates the task of notifying people when a quiz is ready for review or newly published. The email feature creates an email message that includes a link to the quiz and populates the recipient field with those users and groups that have access to the quiz. Before sending the message, you can customize the message to your requirements. Use the following procedure to send an email notification for a quiz.

Notes

- VPC requires configured mail server information before allowing you to use the email feature. For more information, see "Configuring VPC to Use a Mail Server."
- To require email notifications for all review or published documents, use the **Automate E-mail Notification** options when configuring mail server information.

To send a document notification:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. On the Review or Published tab, select the appropriate quiz and click **E-mail**.

   The E-Mail window opens.

3. *Optional*. Modify the **From**, **To**, **Subject**, **Cc**, and **Bcc** fields as appropriate.
4. For **Message Text**, in the URL located in the third paragraph, replace localhost with the name of the server hosting VPC.

   Note
   The email message includes the URL as an active hyperlink.

5. Delete the first paragraph of the message text, and modify the message if appropriate.
6. Click **Submit** to send the notification.

   VPC displays a confirmation that the email was sent successfully.

7. Click **Close** to return to the View/Edit Quiz page.

Organizing Quizzes

VPC supports setting folders to store similar policy documents and quizzes. For example, you can create a folder named “Email Documents” and include an email policy and the related quiz. VPC also supports archiving documents, which removes the documents from view in the User Site but saves the documents for reference and future use.

Note
NetIQ Corporation recommends developing a folder structure and naming scheme before you begin importing and creating documents. For more information, see “Organizing Documents.”

Adding Quizzes to Folders

Once you set up your folders, you can add policies and quizzes in the draft, review, or published phase. You cannot add an archived document to a folder because a document is archived in the folder where the document resides when the archiving action occurs. Use the following steps to add a quiz to a folder.

Notes

- For information about creating folders, see “Creating Folders.”
- If you are updating VPC from a previous version, VPC assigns to the root folder all quizzes previously not assigned to a folder.

To add quizzes to a folder:

1. On the Education tab, click **View/Edit Quiz**.
2. Select the appropriate quiz, and then click **Add To**.

   VPC displays the Folder page.
3. Click **Quizzes** under the appropriate folder, and then click **Save**.
4. Click **Close** to return to the View/Edit Quiz page.

Exporting a Quiz

You can export quizzes into XML format files and store or archive the files outside of VigilEnt Policy Center. Use the following steps to export a quiz.

To export a quiz:

1. On the Education tab, click **View/Edit Quiz**.
2. On the appropriate tab, select the quiz for export, and then click **Export**.

   VPC displays the Export dialog box.
3. Click **Export**, and then follow the steps in the wizard to export the file.

Archiving a Quiz

Archiving a quiz removes the quiz from view in the User Site and saves the quiz for reference and future use. Save time when creating a quiz similar to an archived quiz. Copy the archived quiz and make the necessary changes to create a new quiz. For more information about copying and editing a quiz, see “Using a Template or Sample to Create a Policy Document.” Use the following steps to archive a quiz.

To archive a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. On any tab, select the quiz for archiving, and then click **Archive**. VPC displays the quiz on the Archived tab, and users can no longer see the quiz on the User Site.

Viewing a Quiz

You can view a quiz in any stage of its life-cycle. The procedures are the same when viewing a quiz from any of the View/Edit Quiz and Quiz Library lists. Perform the following steps to view a quiz.

To view a quiz:

1. On the Education tab, click **View/Edit Quiz**.

   VPC displays the View/Edit Quiz page.

2. Select the quiz for viewing, and then click **View**.

   VPC displays the Quiz Preview page.

3. Scroll the quiz to view each question and its answers.
4. Click **Close** to return to the View/Edit Quiz page after viewing the document.

Chapter 10
Implementing Incident Reporting

Incident Reporting allows you to analyze and manage trends in policy violations and erroneous activity. In addition to addressing regulator concerns, incident reporting helps ensure that your existing policies and procedures are understood and effective.

The VPC Incident Reporting feature allows you to set up incident administrators and customize the reporting form to meet the requirements of your organization. After you set up Incident Reporting, any VPC user can report an incident from the User Site.

Note
Reporting incidents in VPC does not count against the VPC user license.

Setting Incident Reporting

Setting Incident Reporting involves defining incident response administrators and customizing the form used to report incidents. You can set up incident response groups to restrict VPC access to only those permissions necessary to manage incident reports. You can also set up incident administrators and assign them to specific types of incidents so VPC notifies the administrators only when someone reports an assigned incident. The report form provides options to specify unique incident types and actions to take when someone or something creates an incident.

Creating an Incident Response Group

You may want to create a group with the responsibility of managing and acting upon incident reports. Grant this group access to only those permissions necessary to manage incident reports. Creating an incident response group includes creating a role, adding users, and then adding permissions. Use the following steps to create an incident response group.

To create an incident response group:

1. On the Administration tab, click **Users**, and then click **Role Info**.

   VPC displays the Role Info tab as shown in the following figure:

2. On the Role Info tab, click **Add**.

   VPC displays the Role dialog box.

3. Type `Incident Administrators` in both the **Role Name** and **Description** fields.

4. Click one of the **Add** icons to add a new user or group.

5. In the **Search for Users** or **Search for Groups** field, type the name of the account that you want to add to the role, and then click **Search**. You can search for all users or groups by clicking **Search** without making an entry in the search field.
6. Click the appropriate entry from the displayed list. To select more than one entry, press **CTRL**, and then click to select non-consecutive entries. Press **SHIFT**, and then click to select consecutive entries.
7. Click **Submit**.

   VPC displays the selected users on the Role page.
8. Verify that the Role dialog box contains the correct users, and then click **Save**.
9. Verify the role by clicking **Search** with a clear **Search for Roles** field.

To add permissions to the incident administrator role:

1. On the Administration tab, click **Permissions**, and then select **Incident Administrators** from the **Role/User/Group** field.

   The Permissions page displays the current permissions for the Incident Administrators.
2. Expand the **All Permissions** check box, and then expand the **Administration** check box.

   VPC displays more permissions.
3. Select the **Incident Reporting** check box, and then click **Update**.

   VPC displays a verification message.
4. Click **OK**.

Adding an Incident Reporting Administrator

You can assign specific administrators to certain types of incidents and select whether VPC notifies administrators by an email message when a user reports an incident. Use the following instructions to set up an incident reporting administrator.

To add an incident reporting administrator:

1. On the Administration tab, click **Incident Reporting**.

   VPC displays the Incident Administrators page.
2. Click **Add**.

   VPC displays the Administrator Information page.
3. In the box next to **Search**, type the first few characters of the name of the administrator and then click **Search**.
4. Select the user from the list of results.
5. Type the information in the **E-mail**, **Extension**, and **Office Location** fields.

   Note
   If you leave the **E-mail** and **Extension** fields blank, after you click **Save,** VPC attempts to populate the fields with data from the user repository.

6. Click one or more incident types from the **Responsibilities** list. To select more than one type, press **CTRL**, and then click to select non-consecutive types. Press **SHIFT**, and then click to select consecutive types.

Note
Select at least one incident type from the **Responsibilities** field for VPC to notify the email address in the **E-mail** field about security incident reports. If you do not select a type, VPC does not send the security officer any email notification when a user submits a security incident report.

7. Select the **E-mail Incident** check box to notify the security officer of an incident.
8. Click **Submit** and VPC displays each administrator's email account, phone number, office location, and the types of incidents for which each is responsible.

Adding a New Type of Incident, Action Required, or Status

The incident report form includes lists with pre-defined choices for reporting the type of incident, the action required, and the status of the incident.

Type of Incident

Helps pinpoint the types of incidents that occur and lets you define to whom VPC sends specific types of incidents for action.

Action Required

Defines what steps an administrator should perform to remedy the incident.

Status

Lets an administrator or user know in what state an incident is at any time.

The choices for these items help guide users through the process of reporting an incident. You can customize the lists by adding and deleting choices. Use the following instructions to add a choice to a list in the incident report form.

To add a new incident type, required action, or status:

1. On the Administration tab, click **Incident Reporting**, and then click **Options**.

   VPC displays the Incident Report Options dialog box.

2. Click + next to the list for **Type of Incident**, **Action Required**, or **Status**.
3. Type the name for the new choice in the **Option** field, and then click **Submit**.

   VPC displays the new choice in the appropriate list. You can delete information in the lists by clicking the option you want to delete, and then clicking **X**.

4. Click **Update** to save the change.

Showing and Hiding Fields in the Incident Report Form

VPC allows you to hide or show the **Action Required**, **Affected System Details**, and **Location of Problem** fields in the incident report form. Use the following procedure to show or hide the fields.

To customize the incident report form:

1. On the Administration tab, click **Incident Reporting**, and then click **Options**.

   VPC displays the Incident Report Options dialog box.

2. *Optional.* To display the **Action Required** list, click **On**.

   Action Required allows user to select from a list of actions required to address the incident. VPC uses the actions specified in the **Action Required** list.

3. *Optional.* To display the **Affected System Details** fields, click **On**.

   Affected System Details displays several fields to report the details of the computer affected by the incident. The fields include IP address, type of operating system, manufacture, serial number, corporate property number, and type of system connection (network or modem).

4. *Optional.* To display the **Location of Problem** fields, click **On**.

   Location of Problem displays fields to describe the physical location of where the incident occurred. The fields include address, room, and building.

5. Click **Update** to save the changes.

Configuring Anonymous Incident Reporting

Anonymous incident reporting lets users report all or only specific types of incidents without adding user-identification information. This option lets users report an incident without fear that they may be incriminated or suffer adverse retribution from the incident being reported. Use the following information if you want to set up anonymous incident reporting in your organization.

To configure anonymous incident reporting:

1. On the Administration tab, click **Incident Reporting**, and then click **Options**.

   VPC displays the Incident Report Options list.

2. Click **On** in the **Enable Anonymous Incident Reporting** field.

3. *Optional.* To select the types of incidents for anonymous reporting, click **Options**, select the appropriate report types, and then click **Save**.

   VPC displays the selected options under **Active Anonymous Incident Report Types**.

4. Click **Update** to save the anonymous settings.

Submitting an Incident Report

You can submit an incident report from the Reporting tab on the Administration Site or by a user on the User Site. The following steps provide instructions on submitting an incident report from the Administration Site.

Note

You can customize the incident report form by showing or hiding fields (see “Showing and Hiding Fields in the Incident Report Form”) or by modify the choices in lists (see “Adding a New Type of Incident, Action Required, or Status”).

To submit an incident report:

1. On the Reporting tab, click **Incident Reporting**, and then click **Report**.

   VPC displays the Incident Report form.

2. *Optional.* Under **Contact Information**, verify your name, phone number, fax number and email address.
3. Under **Incident Information**, for **Type of Incident**, select the kind of incident included in this report. For example, if the security incident involved a person accessing a secure area illegally, you may select a choice such as **Unauthorized Access**.
4. For **Brief Description**, type a description of the incident that occurred.
5. *Optional.* Type the information for **Date/Time Details**, **Location of Incident**, and **Additional Contacts Information**.
6. *Optional.* For **Action Required**, select the action necessary to resolve this incident. For example, if you create a report only to note that an event occurred, you may select a choice such as **Report Only**. If you create a report to solve a problem with someone easily entering a secure area, you may select a choice such as **Update** or **Fix**.
7. *Optional.* For **Action Taken**, select the action performed to resolve this incident. For example, if the matter has been resolved already, select a choice such as **Resolved**. Or, if you have taken only this first step, you can select a choice such as **Reported**.
8. *Optional.* For **Status**, select the current status of the incident.
9. *Optional.* For **Time Spent on Handling**, type the amount of time, in hours, spent on this incident.
10. *Optional.* Under **Affected System Details**, if the incident affects a computer, type the computer information.
11. *Optional.* Under **Location of Problem**, type the address, room, and building in which the incident occurred.
12. Click **Submit** and VPC displays the tracking number for this report.

Managing Incident Reports

As an incident progresses, incident administrators can update the status and add notes and details. Incident administrators may also want to export the reports to an Excel worksheet.

Viewing an Incident Report

Before submitting a security incident report, an administrator may want to see if similar reports already exist. VPC assigns all security incident reports a tracking number used to find the exact report you want. Use the following steps to search for and view existing security incident reports.

Note
Only those incident types to which an administrator has been given explicit responsibility show in the **Type of Incident** field.

To view an incident report:

1. On the Reporting tab, click **Incident Reporting**, and then click **Search**.

   VPC displays the Search Database page.

2. Type any search criteria in the appropriate field, and then click **Submit**.

   VPC displays the Results list.

3. Click the ID number of the report to view the report on the History page.

Editing an Incident Report

As the resolution of an incident report progresses, administrator may want to update the status or include more detail to a report. Use the following steps to edit a security incident report.

To edit an incident report:

1. On the Reporting tab, click **Incident Reporting**, and then click **Search**.
2. Type any search criteria in the appropriate field, and then click **Submit**.

   VPC displays the Results list.

3. Click the tracking number of the report to view the report on the History page.
4. Click next to the tracking number of the incident, and then click the **Edit** icon.

   VPC displays the incident on the Incident Response page.

5. Make any changes, and then click **Submit**.

Exporting an Incident Report

An organization may want to save security incident reports in a format or location outside of VigilEnt Policy Center. VPC lets you export a report to Microsoft Excel format for you to save in a chosen location. Use the following steps to export an existing security incident report.

To export an incident report:

1. On the Reporting tab, click **Incident Reporting**, and then click **Search**.
2. Type any search criteria in the appropriate field, and then click **Submit**.

   VPC displays the Results list.

3. Click next to the tracking number, and then click the **Export** icon.

   The computer displays the File Download window.

4. Click **Save**.

   The computer displays the Save As window.

5. Select the appropriate storage path, rename the file in the **File name** field, and then click **Save**.

Chapter 11

Customizing the User Site

The User Site exists as a central location to distribute information security procedures, general news items, and receive feedback from users. This information is disseminated throughout the organization to each employee based on user ID. From the User Site, users can read policy documents, complete quizzes, and view news items posted by the administrator. If you set certain permissions, users can create their own account, modify the account information, change their password, report a policy violation, and change the language in which VPC displays their home page.

Note

For information about performing tasks in the User Site, see the User Site Help.

Using Frames

The User Site contains a news frame to post information for your employees. An additional, customizable frame is also available if you select to configure and display it.

Using the News Frame

The news frame within the User Site can carry any information that your organization wants the employees to know. You can use the news frame to alert users of a new policy document or quiz, warn them of potentially damaging email message viruses, or remind users of an upcoming holiday. Use the following steps to personalize the news frame.

To use the news frame:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, clear the **Hide the NEWS frame on the User Site** check box.
3. Click **Update** and the User Site includes the news frame.

To hide the news frame:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, click **Hide the NEWS frame on the User Site**.
3. Click **Update** and the User Site does not include the news frame.

Using the Custom Frame

The lower part of the User Site is the custom frame. This area can contain any information, such as a link to the company Web site. You can remove the frame if this information is no longer wanted. If you want the information displayed for a specific period of time, use the news frame feature as described in “Using the News Frame.” Use the following steps to personalize the custom frame.

To use the custom frame:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, clear **Hide the CUSTOM frame on the User Site**.
3. In the custom area, type the appropriate information using HTML commands.
4. Click **Preview** to view an example of the User Site.
5. Click **Update** and the User Site includes the custom frame.

To hide the custom frame:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, click **Hide the CUSTOM frame on the User Site**. This option hides the information in the custom frame on the Home page, but does not remove the information from the custom area on the Design tab.
3. Click **Update** and the User Site does not include the custom frame.

Using a Targeted Frame

Users may be more comfortable using VPC in a familiar format, such as your intranet. If your intranet lets you launch applications in a targeted frame, you can set up VPC to function within that environment.

To deploy VPC in a targeted frame:

1. Log on to the Administration Site.
2. On the Administration tab, click **User Site**.
3. Click **Deploy VPC within a targeted frame**.
4. Type the name of the frame in which you want to display VPC. You can find the name in your HTML source code as shown in the following example, where the targeted frame name is `AppFrame`:

   ```
   <frame src="http://vpcServerName:8080/policy" name="AppFrame" id="AppFrame" ...>
   ```

5. Click **Update**.

Using Custom Styles

You can customize the following features of the User Site:

- The page that displays upon opening
- The title bar text

- Fonts and colors, using VPC options or a custom style sheet
- Comment boxes and confirmation text
- The order in which documents display

Customizing the User Site Initial View

You can set your organization's User Site to display the Home page or My Document page after a user successfully logs on to VPC. Set your User Site to display the My Document page if you want your users to see all of their documents at once rather than only those that they have not yet read, as shown in the Home page. Customize the User Site initial view by using the following steps.

To customize the User Site initial view:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. Click **Load home page after successful logon** to view the Home page when you log on to the User Site or click **Load My Documents page after successful logon** to view the My Documents page when you log on to the User Site.

3. Click **Update**.

Customizing the User Site Title Bar

The title bar is the uppermost text on the User Site browser. You can customize this area to display any text including your company's name, location, or motto. Use these steps to customize the title bar.

To customize the title bar on the User Site browser window:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. Edit the text in the **Titlebar text** field.

3. Click **Update** and VPC changes the User Site information.

Customizing the Basic Style Options

VigilEnt Policy Center includes some color and font styles so that you may change the User Site. If you have your own style sheet including your logo, colors, and fonts, use the instructions in "Adding a Custom Style Sheet" to set up your User Site. Use the following steps to change the look of your User Site using a preset color and font.

To change the basic preset color or style themes:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, under **Style Options**, click the **Preset Color Theme** and **Preset Style Theme** that you want to display on the User Site Home page.

3. Click **Preview**.

   VPC displays an example of the User Site in a separate window.

4. Close the preview window, and then click **Update** and VPC changes the User Site from the default colors and font.

Adding a Custom Style Sheet

If your organization has its own style sheet that includes colors and fonts different to those provided with VigilEnt Policy Center, you can add the information to the User Site. The custom theme helps to adapt the User Site to your overall organization image by sharing the similar use of color and font.

To upload a custom image:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, under **Style Options**, click **Advanced**, and then click **Launch**.

   VPC displays the Advanced Design Options page.

3. Under **Header Customization**, click **Upload a custom header image** to use a particular image as the User Site header, and then type the image file's location in the clear field.

   Note
   VPC requires a custom header image size of 750px by 69px. If you use a different dimension, VPC skews the image to fit the space and displays the image improperly.

4. *Optional*. Type a color in hexadecimal format in the Background Color field. VPC uses this color as the background for the custom header.

5. Click **Save**.

   VPC displays the message window.

6. Click **Close**.

7. Click **Update** and VPC changes the User Site information.

To create a custom header using HTML:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, under **Style Options**, click **Advanced**, and then click **Launch**.

   VPC displays the Advanced Design Options page.

3. Under **Header Customization**, click **Type the HTML to be used as the custom header** to use HTML to design a particular User Site header.

4. In the custom area, type the information that you want to display in the custom header by using HTML commands.

5. Click **Save**.

   VPC displays the message window.

6. Click **Close**.
7. Click **Update** and VPC changes the User Site information.

To use custom colors and fonts:

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the Design tab, under **Style Options**, click **Advanced**, and then click **Launch**.

   VPC displays the Advanced Design Options page.

3. *Optional.* Type a color in hexadecimal format in the **Background Color** field. VPC uses this color as the background for the User Site including the Document Reader window.
4. *Optional.* Type a color in hexadecimal format in the **Text Color** field. VPC uses this color as the text for the menu bar and footer.
5. *Optional.* Type a font name in the **Font-family** field.

   VPC uses this font as the text style.

6. Click **Save**.

   VPC displays the message window.

7. Click **Close**.
8. Click **Update** and VPC changes the User Site information.

Customizing the Comment and Confirmation Panes

By default, the page in the User Site that displays documents has three panes:

- The *Document* pane, located at the top of the page, displays the policy or quiz.
- The *Comments* pane, located in the middle of the page, provides an area for users to add a comment to a document in review or published state.
- The *Confirmation* pane, located at the bottom of the page, provides a check box for users to acknowledge that they have read or reviewed the document. For quizzes in Published state, the Confirmation pane shows the passing or failing quiz score.

You can show or hide the Comments pane, allow reviewers to see the review comments of other reviewers, or modify the text in the Confirmation pane. Use the following steps to customize the Comments and Confirmation panes on the document viewer page.

To customize the Comment and Confirmation panes:

1. On the Administration tab, click **User Site** and then click the Info tab.
2. Under **Comments From Users**, to display the comments pane for published documents, click **On**. If the option is **Off**, users cannot send online comments.
3. Under **Comments From Reviewers**, to display the comments pane for documents in Review state, click the first **On** option. If the option is **Off**, reviewers cannot send online comments.
4. Under **Comment From Reviewers**, to display a View button in the comments pane for documents in Review state, click the second **On** option. If the option is **Off**, reviewers cannot view comments of other reviewers.

5. In the **Policy Confirmation Text** field, accept the default text or type the text to display for users to acknowledge that they have read and understood a policy.

6. ***If you want to add a translated copy of the confirmation text for display on the User Site***, complete the following steps:

   a. Click the **Languages** link for the Published confirmation text.

   b. Select a language for which to enter translated text and click **Add**.

   c. Enter the translated text associated with the designated language.

   d. Click **Save** on the menu bar to commit the text entry to the database.

      Users who log on to VPC with an interface language selection that matches the language of the confirmation text will see the translated copy of the text.

   e. To remove a language equivalent copy of the confirmation text, select the text you want to delete and then click **Delete**.

   f. Click **Cancel** on the menu bar to close the window and return to the Info page.

7. In the **Review Policy Confirmation Text** field, accept the default text or type the text to display for users to acknowledge that they have reviewed the document.

8. ***If you want to add a translated copy of the confirmation text for display on the User Site***, complete the following steps:

   a. Click the Languages link for the Review confirmation text.

   b. Select a language for which to enter translated text and click **Add**.

   c. Enter the translated text associated with the designated language.

   d. Click **Save** on the menu bar to commit the text entry to the database.

      Users who log on to VPC with an interface language selection that matches the language of the confirmation text will see the translated copy of the text.

   e. To remove a language equivalent copy of the confirmation text, select the text you want to delete and then click **Delete**.

   f. Click **Cancel** on the menu bar to close the window and return to the Info page.

9. Click **Update** and VPC updates the User Site with your entries.

Selecting Document Sorting Options

You can select the default order in which documents display on the Home and My Documents pages of the User Site. Sort orders include alphabetical, or by the document creation, publication, or available dates. Users can change the sort order after accessing the User Site. Use these steps to select an order.

To select a document sort option:

1. On the Administration tab, click **User Site**, and then click the Info tab.

   VPC displays the Info tab.

2. Under **User Site Document Display Options**, click the option by which you want to sort documents on the User Site, and then click **Update**.

   Note
   The **Default** sort puts documents in the order in which they return from the database, which is different server-to-server and may seem that VPC is randomly displaying documents on the User Site. However, the Default sort returns information faster than the other sort options because VPC returns the data quickly and does not arrange the information. If you have a large number of documents, you may sacrifice performance when using one of the other sorting options.

3. Check the User Site to verify that VPC displays all available policy documents and quizzes in the selected sort order.

Setting User Site Privileges

You grant User Site permissions by showing or hiding items in the User Site. For example, if you want to allow users to report incidents from the User Site, you set VPC to display the Incident Report icon on the User Site.

There is a great deal of flexibility when setting permissions for users, so be sure to review each available privilege for the User Site.

To set permissions for the User Site:

1. On the Administration tab, click **User Site**, and then click **Privileges**.

   VPC displays the User Site page with the Privileges tab on top.

2. Select whether to show the Account Creation icon on the Log On page of the User Site. The Account Creation icon gives users access to enter the information necessary to create their own account. If the icon is not available, administrators can create user accounts.

   Note
   If you use an external source for the user repository, you cannot create user accounts in VPC. You should create and maintain user accounts through the user manager utility of the external source. For more information, see “Understanding Deployment Options.”

   - To show the Account Creation icon on the User Site, click **Permit all users to create their own accounts**.
   - To hide the Account Creation icon on the User Site, click **Restrict access to user account creation**. Select this option if you use an external source for the user repository.

3. Select whether to show the My Information icon, which allows users to update their name, email address, department, and extension. If this icon is hidden, administrators can update this information.

   Note
   If you use an external source for the user repository, you cannot edit user accounts in VPC. You can create and maintain user accounts through the user manager utility of the external source. For more information, see “Understanding Deployment Options.”

   - To show the My Information icon, click **Permit all users to edit their personal information**.
   - To hide the My Information icon, click **Restrict access to user information edits**. Select this option if you use an external source for the user repository.

4. Select whether to show the Report Incident icon, which gives users access to the Incident Report form so any VPC user can report policy violations and erroneous activity.

   Note
   Using Incident Reporting does not count against the VPC user license.

   - To show the Incident Report icon, click **Permit all users to report incidents**.
   - To hide the Incident Report icon, click **Restrict access to incident reporting**.

5. Select where to display a user’s score after they take the quiz. VPC can display the resulting score on the My Documents page of the User Site so a user can view their quiz score. VPC can also display the score on the User Report so administrators can view the score.

   - To show a user’s quiz score on the My Documents page of the User Site and on the User Report, click **Activate all passing grade functionality**.
   - To hide the user’s quiz score on the My Documents page of the User Site, but show the score on the User Report, click **Activate passing grade functionality**.
   - To hide a user’s quiz score on the My Documents page of the User Site and on the User Report, click **Deactivate all passing grade functionality**.

6. Select how to display a quiz grade:

   - To show the grade as a percentage of correct answers, click **Display passing grade as a percentage**.
   - To show the grade as pass (P) or fail (F), click **Display passing grade as a lettered value**.

7. Select whether to show the language list within the User Site menu bar. The language list allows users to select the language of the text in the User Site. Available languages include Dutch, English, French, German, Portuguese, Spanish, and Swedish.

   - To display the language list, click **Permit user to select an interface language**.
   - To hide the language list, click **Do not permit users to select an interface language**.

8. Select whether to show a Password box after the confirmation message in the document reader dialog box. Requiring a user to enter a password after confirming that they have read or reviewed a document ensures that the person who acknowledges is truly the user.

   - To display the Password box, click **Activate electronic signature on user acknowledgement of documents read or reviewed**.
   - To hide the Password box, click **Deactivate electronic signature on user acknowledgement of documents read or reviewed**.

   Note
   Electronic signatures work with logging. Therefore, to display the electronic signature feature on the User Site, you also can enable the **Documents electronically signed** setting under **Policy Document Options**. For more information about setting logging options, see "Setting Audit Logging."

   ---

9. Select whether to show the **Properties** button on the document reader window for documents posted for review. The **Properties** button allows reviewers to see information such as document author, active date, and other general information about the document.

   - To show the **Properties** button, click **Permit users to view policy and quiz properties for documents in review**.
   - To hide the **Properties** button, click **Do not permit users to view policy and quiz properties for documents in review**.

10. Click **Update** and VPC changes the User Site permissions.

Managing News Items

After creating a policy document and quiz, you can add a news item to the User Site reminding employees to read the policy and complete the quiz. News items include helpful tips, such as knowing the building evacuation plan, or a reminder of a blood drive in the building.

Posting a News Item

After creating a policy document and quiz, you can add a news item to the User Site reminding employees to read the policy and complete the quiz. News items include helpful tips, such as knowing the building evacuation plan, or a reminder of a blood drive in the building. The following steps walk you through posting a news item.

To post a news item:

1. On the Administration tab, click **User Site**, and then click the News tab.

   VPC displays the News tab.

2. On the New tab, click **Add**.

   VPC displays the News Item dialog box.

3. Type the number in the **Order Index** field to correspond with the order in which VPC displays news items when more than one item exists.

4. Select the **Show News Item** check box. You can clear this check box to keep the news item on file yet prevent the item from displaying on the User Site.

5. Verify that the **Available From** date and **Available To** dates. You can set the **Available To** date to the same day, or any future date, as the **Available From** date.

6. Type the news information in the **Text** field.

7. Click a language from the **Text Language** list. This selection should match the language selection in the User Site for the information to display.

   You can include news items for more than one language using the **Text Language** list. For example, type the English text and click **English** before saving the item. Create the same news item in German and click **German**. VPC displays the German news item for users who have **German** selected as their language.

8. Click **Save** and the User Site displays the news item in the news frame.

Adding an ACL to a News Item

1. On the Administration tab, click **User Site**.

   VPC displays the User Site page.

2. On the News tab, select the appropriate file, and then click **ACL**.

   VPC displays the Access Control List dialog box.

3. Click the appropriate access from the **Available Privileges** field, and then click **>>** to move the privilege to the **Selected Privileges** field.

4. Click **Save**.

Hiding a News Item

1. On the Administration tab, click **User Site**. VPC displays the User Site page.

2. On the News tab, click the news item that you want to hide.

3. Click **Hide/Show**.

   VPC hides the information in the news frame on the Home page.

4. Verify the information is still on the News tab. A check mark in the **Active** field shows the available news items where an empty **Active** field shows that the news item is hidden or the current date is not within the available date range.

Chapter 12

Managing Reporting

This chapter includes details about the reporting tools available in VPC. You can export reports to Microsoft Excel, and you can display the results in multiple formats. The reporting Dashboard shows administrators and compliance managers a snapshot of your current compliance and allows you to quickly access statistics on a particular document.

Note

An “available document” is defined as a document in the Review or Published state that has users assigned to the document using an access control list, and one in which you have Manage privileges.

Using Compliance Reporting

VPC offers a variety of reports to track and manage policy compliance. The Compliance Reporting area allows you to run compliance and exception reports on all available documents in review and published states within VPC as long as users are assigned to the document. You can also run user reports including single user summary reports and multiple user summaries.

Understanding the Dashboard Tab

The anchor of compliance reporting within VPC is the Dashboard tab. This tab includes the summary Report area, Progress Report area, and Report Wizard. When you access the Dashboard tab, VPC populates the tab with current numbers on your documents and users. Although you cannot print reporting information from the initial Dashboard page, you can use the print feature once you go into more detail for a particular report.

The Dashboard tab includes the following components:

Summary Report

The Summary Report area displays statistics for all of your available documents, including a pie chart representation each for your current enterprise, policy, and quiz compliance.

- **Enterprise Compliance —** Displays the total number of available documents, number of users required to acknowledge those documents, and the percentage of users who are compliant. Click in the Enterprise Compliance area to access the Summary Report details for all your available documents.
- **Policy Compliance —** Displays the total number of available policy documents, number of users required to read those documents, and the percentage of users who are compliant. Click in the Policy Compliance area to access the Summary Report details page for your available policy documents.

- **Quiz Compliance —** Displays the total number of available quizzes, number of users required to complete those quizzes, and the percentage of users who are compliant. Click in the Quiz Compliance area to access the Summary Report details page for your available quizzes.

Progress Report

The Progress Report area includes all available documents, including policy documents and quizzes in the review or published state. Click the title of a document and VPC displays a high-level summary report for that document.

Report Wizard

The Report Wizard offers a limited report configuration and allows you to quickly run a basic report. Click **Expand** in the Report Wizard area and VPC displays the Configure tab for you to create a report with more specific parameters.

To access the Dashboard tab:

1. Access the Administration Site.
2. Click Reporting and then click Compliance Reporting. VPC displays the Dashboard tab with a snapshot of your current enterprise compliance.

Note
If VPC does not display a certain document, verify that the document is in the Review or Published state and has users assigned, using an access control list, to review or read the document.

Running Detailed Summary Reports

VPC offers summary reports for your entire enterprise, policy documents, or quizzes. All summary reports include the % **Compliant**, **Owner**, **Title**, **Total Users**, and **Responses**. The detailed Enterprise Compliance report includes the report **Type**, whether it is a policy or quiz. The detailed Policy Compliance report includes **Time in State** for the number of days the document is in the Review or Published state. The detailed Quiz Compliance report includes the **Average Score** based on the number of users who have completed a quiz. Use the following steps to run a Detailed Summary Report.

To run a Detailed Summary Report:

1. Access the Administration Site.
2. Click **Reporting** and then click **Compliance Reporting**.

   VPC displays the Dashboard tab with a snapshot of your current enterprise compliance.
3. ***If you want to run a detailed summary report for your enterprise,*** click the pie chart in the Enterprise Compliance area.

4. ***If you want to run a detailed summary report for your policy documents,*** click the pie chart in the Policy Compliance area.
5. ***If you want to run a detailed summary report for your quizzes,*** click the pie chart in the Quiz Compliance area

Notes

- You can send an email message to the document owner by selecting the check box next to the **Owner**, and then clicking **Email**. Type the appropriate message in the **Message Text** box, and then click **Submit**.
- You can send the report results to Microsoft Excel for management by clicking **Export to Excel** and following the prompts.

Running Detailed Progress Reports

VPC includes detailed progress reports for all your available documents. For each user, VPC displays the **Date Taken**, **UserID**, **First Name**, and **Last Name**. Use the following steps to run a Detailed Progress Report.

To run a Detailed Progress Report:

1. Access the Administration Site.
2. Click **Reporting** and then click **Compliance Reporting**.

   VPC displays the Dashboard tab with a snapshot of your current enterprise compliance.
3. Click the title of the document for which you want to run a report.

Notes

- You can send an email message to the document owner by selecting the check box next to the **Owner**, and then clicking **Email**. Type the appropriate message in the **Message Text** box, and then click **Submit**.
- You can send the report results to Microsoft Excel for management by clicking **Export to Excel** and following the prompts.

Using the Report Wizard

VPC includes a Report Wizard on the Dashboard tab for you to run quick and simple document reports. Use the Configure tab to set more parameters for a report. Use the following steps to run the Report Wizard.

To run a report using the Report Wizard:

1. Access the Administration Site.
2. Click **Reporting** and then click **Compliance Reporting**.

   VPC displays the Dashboard tab with a snapshot of your current enterprise compliance.
3. In the **Report** field, select the type of report you want to run.
4. In the **Title** field, select the title of the document for which you want to run the report.
5. In the **Scope** field, select **Users/Groups in ACL**.
6. In the **Type** field, select the type of report you want, and then click **Run**.

Re-Running Compliance Reports

VPC offers the ability to re-run individual compliance reports with previously specified criteria without having to re-enter the criteria each time.

Note

This feature is available only for compliance reports that you configure after installing or upgrading to VPC 5.6. If you have reports that you ran frequently in earlier versions of the product, you should recreate them in VPC 5.6 so you can re-run them.

To re-run a compliance report:

1. Follow the same steps to configure and run the report as in previous versions of the product. For more information, see "Using the Report Wizard" on page 139.
2. On the Reporting tab, click the View tab.
3. Select the report you want to re-run and then click the **Report Rerun** icon.
4. Repeat these steps for each report you want to re-run. VPC does not currently offer the ability to re-run multiple reports at the same time.

Viewing Reports

Once you have run reports, you can view the results using the View or Archive tab. By storing reports on their own page, VPC lets you view the results easily from one location. Use the following steps to view your reports.

To view a report:

1. Access the Administration Site.
2. Click **Reporting** and then click **Compliance Reporting**.

   VPC displays the Dashboard tab with a snapshot of your current enterprise compliance.
3. Click **View** or **Archive**.

   VPC displays the appropriate tab containing all available reports for which you have permission to view.
4. Click the appropriate report to view the contents.

Chapter 13

Administering VPC

The Administration Site contains several options and features to help you administer VPC to meet your organization's specific security and auditing needs.

Viewing Information about VPC

The About page contains license, copyright, trademark, and configuration information. You can also check for the latest version of VigilEnt Policy Center and view any third-party licenses. The steps in the following tasks help you use the About page.

To check for the latest version of VigilEnt Policy Center:

1. On the Administration tab, click **About**.

   VPC displays the About page.

2. Click **Version** to view information about the most recent version of VPC available.

To view third-party license agreements:

1. On the Administration tab, click **About**.

   VPC displays the About page.

2. Click **Third-Party License Agreements**.

To view your system configuration:

On the Administration tab, click **About** and VPC displays the About page. The System Configuration area contains the following fields:

- **VPC Server Port**: Displays the port number of the server where VPC receives requests for data.
- **VPC Shutdown Port**: Displays the port number of the server where VPC receives requests for stopping the service.
- **VPC Agent Port**: Displays the port number of the server where VPC receives requests from Vulnerability Manager (VM users only).

Updating a License

When an administrator logs on to the Administration Site, VPC displays a license expiration warning message if the license expires within the next 30 days. As an additional warning, a power user receives the same license expiration warning message when attempting to log on to the User Site. The administrator and power user can continue on to the Administration Site and User Site after clicking **OK**.

Organization receives a new license key upon payment of the product renewal. Use the following steps to update your license key and verify the licensing information.

Note
To learn more about VPC licensing, see “Understanding Licensing.”

To update a license:

1. On the Administration tab, click **Options**, and then click **License**.

   VPC displays the License tab.

2. Type the license key in the **New License Key** field.
3. Click **Update**.

To verify a license:

1. On the Administration tab, click **About**.

   VPC displays the About VigilEnt Policy Center page.

2. Verify the information on the page. Contact NetIQ Technical Support if you believe that the displayed information is incorrect.

Viewing an Audit Log

If you have set VPC to log audit information to a file, use the following steps to view your audit logging stored in that file.

Note
VPC logs an action only after logging has been activated for that action. For more information about audit logging, see “Setting Audit Logging.”

To view the audit log file:

1. On the Administration tab, click **Options**.

   VPC displays the Options page with the Log tab on top.

2. Under **Audit File Path**, click **View** and VPC displays the file.

Increasing Your Temporary Internet Disk Space

In some situations, increasing your temporary Internet disk space may improve the performance of the Administration Site. Increase your temporary Internet disk space by using the following steps.

To increase your temporary Internet disk space:

1. Open your Web browser.
2. From the **Tools** menu select **Internet Options**.

   The browser displays the Internet Options dialog box.
3. Click **Settings**.

   The browser displays the Settings dialog box.
4. Type `100` in **Amount of disk space to use**.
5. Click **OK**, and then click **OK**.

Running Admin Reports

VPC offers several reports to help you administer VPC. You can export each report to Microsoft Excel.

Running an Access Control List Report

VPC offers two ACL reports to help you administer access control lists.

- The ACL Membership Report lists the users, groups and permissions associated with each ACL.
- The ACL Document Report lists the documents associated with each ACL.

You can run ACL reports for all ACLs or for a specific ACL. Perform the following steps to run an ACL report.

To run an ACL report:

1. On the Administration tab, click **Admin Reports**, and then click **ACL**.

   VPC displays the ACL tab.
2. *Optional.* ***If you want to run a report that displays hidden ACLs,*** click **Include hidden ACLs as options for single ACL reporting**.

   Note
   Hidden ACLs are ACLs that VPC automatically creates whenever a user other than the main Site Administrator creates a new document, reassigns a document, or applies users directly to a document on the Administration Site.
3. Select the ACL report you want to run:
   - To view users, groups, and permissions associated with an ACL, click **ACL Membership Report**.
   - To view the documents associated with an ACL, click **ACL Document Report**.
4. Under the appropriate report, select the scope:
   - To run a report for all ACLs, click **All ACLs**.
   - To run a report for a specific ACL, click **Single ACL** and then select the appropriate ACL.
5. Click **Report**.

Running an Audit Report

If you set up logging to log to the VPC database, you can run audit reports on any of the actions chosen during logging setup. Once you run an audit report, you can include the information in an email message, print it, or export it as a Microsoft Excel Comma Separated Values file (.csv). Use the following steps to run an audit report.

Notes

- Audit reports show data for only those actions performed *after* the action was configured for logging. For more information about audit logging configuration, see “Setting Audit Logging.”
- An audit button is available on many toolbars so that you can run an audit report while working with an item.

To run an audit report:

1. On the Administration tab, click **Admin Reports**, and then click **Audit**.

   VPC displays the Audit tab.

2. For **Select the item type**, select the type of item you want to audit.

   VPC populates the **Select an item** list with all items available for the selected type.

3. For **Select an item**, select the specific item you want to audit.
4. Click **Report**.

   VPC displays the audit report information for the selected item in the **Narrative** view, sorted **Chronologically**.

5. *Optional.* Change how the information displays in the Report Information dialog box:
   - To sort the information by action, click **Categorical**.
   - To view the information as a table, which can then be exported as a .csv file, click **Dataview**.
6. Click the **X** in the top right corner to close the Report Information dialog box.

Running a Document Report

VPC offers two administration reports to track the status of policy and quiz documents.

- The Master Document Report allows you to view documents by state, such as Draft, Review, Published, or Archived.
- The Document Expiration Report allows you to view documents in Review or Published states within a specified expiration time frame.

Use the following steps to run a document administration report.

To run a Master Document Report:

1. On the Administration tab, click **Admin Reports**, and then click **Document**.

   VPC displays the Document tab.

2. Click **Master Document Report**.
3. Under **Scope**, select which documents to include in the report: **All documents**, **Policies only**, or **Quizzes only**.

4. Under **State**, select the check box next to each state to include in the report.
5. Under **Fields**, select the columns you want to include in the report. You can filter on any of the default fields, as well as on any custom properties you created for your policies and quizzes.
6. Click **Report**.

To run a Document Expiration Report:

1. On the Administration tab, click **Admin Reports**, and then click **Document**.

   VPC displays the Document tab.
2. Click **Document Expiration Report**.
3. Under **Scope**, select which documents to include in the report: **All documents**, **Policies only**, or **Quizzes only**.
4. Under **Report on documents expiring**, click the appropriate time frame.
5. Click **Report**.

Running a Detailed License Report

The Admin Reports License tab shows the total count of licenses for the current VPC license and how many are in use. A user counts toward the license limit and is considered "occupied" if they have read and acknowledged a policy document or completed a quiz within six months from the current date.

For occupied licenses, you can run a report to view details such as the user ID, name, department, and date of last activity. You then have the option to export the report to Excel. Use the following steps to run a Detailed License Report.

To run a Detailed License Report:

1. On the Administration tab, click **Admin Reports**, and then click **License**.

   VPC displays the License tab, which shows the license count.
2. Ensure that **Detailed License Report** is selected.
3. Click **Report**.

Changing Passwords and Company Information

Over time, you may need to change the VPC administration password, database password, or the company information associated with your VPC license.

Changing the Administration Password

You can change the administration password at any time and should change the password regularly to avoid a compromise. Perform the following steps to change the administration password.

To change the administration password:

1. On the Administration tab, click **Options**, and then click **Passwords**.
2. Under **Change VPC administrator password**, type a new password in the **New Admin Password** field and confirm by typing the same password in the **Confirm New Password** field.
3. Click **Update**.

Changing the Database Password

Change the database password when you migrate the database, an administrator changes jobs, or you suspect that the password is compromised. Perform the following steps to change the database password.

To change the database password:

1. On the Administration tab, click **Options**, and then click **Passwords**.
2. Under **Change the database connection password**, type the database password in the **Current Password** field.
3. Type a new password in the **New Admin Password** field and confirm by typing the same password in the **Confirm New Password** field.
4. Click **Update**.

Changing Company Information

Perform the following task to update company information. This information, such as the company name, sets the name in the policy documents when VPC adds content from a sample or library policy document.

To change company information:

1. On the Administration tab, click **Options**, and then click **License**.

   VPC displays the License tab.
2. Type the name of the company in the **Company Name** field.
3. Type the name of the security officer in the **Security Officer** field.
4. Click **Update**.

Uninstalling VPC

You can uninstall VigilEnt Policy Center at any time by using the Add/Remove Programs dialog box provided by Microsoft Windows. The following steps guide you through removing VPC from your computer.

Notes

- If you are using IIS, stop the IIS server before uninstalling VigilEnt Policy Center. VPC does not uninstall properly if you fail to stop the IIS server before attempting to uninstall.
- Uninstalling VPC does not remove the SQL Server database. A database administrator can remove the VPC database tables.

To stop the IIS service:

1. Shut down your Web browser if you are currently running VigilEnt Policy Center.
2. From the **Start** menu, select **Administrative Tools > Internet Information Services Manager**.
3. Right-click the website on which VPC is running (usually the Default Web Site), and then click **Stop**.

To uninstall VigilEnt Policy Center:

1. Shut down your Web browser if you are currently running VigilEnt Policy Center.
2. Open Control Panel and select **Add/Remove Programs**.
3. Scroll the Programs list, and then click **VigilEnt Policy Center**.
4. Click **Change/Remove**.

   The computer displays the Select Uninstall Method dialog box.
5. Click one of the following choices:
   - **Automatic**: Uses the default uninstallation.
   - **Custom**: Allows you to select particular files to remove.
   - **Repair**: Repairs any problems that may have occurred during a previous installation attempt.
6. Click **Next**.

   The computer displays the Perform Rollback dialog box.
7. Click **No** to prevent the computer from restoring any backup files or click **Yes** for the computer to restore backup files, and then click **Next**.

   The computer displays the Perform Uninstall dialog box.
8. Click **Finish**.

   The computer removes VigilEnt Policy Center.
9. Click **Close** in the Add/Remove Programs dialog box.
10. Close Control Panel.
11. Use Windows Explorer to remove any remaining folders and files.