Web Services Guide

NetIQ® VigilEnt™ Policy Center

August 2011

Legal Notice

Contents

About This Book and the Library

The *Web Services Guide* provides conceptual information about the NetIQ VigilEnt Policy Center (VPC) Web Services. This book defines terminology and various related concepts.

Intended Audience

This book helps VPC administrators and internal development teams responsible for implementing VPC Web Services in their organization.

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
Introduction

The demand for better security policy compliance and enforcement increases each day. New privacy considerations and government regulations in health care, financial services, and many other specialized organizations rise to the forefront of concerns. Organizations wanting to stay ahead of newly-introduced electronic commerce initiatives, trusted partner relationships, technologies, and employees implement new information security procedures almost daily.

It is no wonder that more than half of 5,000 respondents to a recent survey did not feel their security policies were in line with business goals. Two-thirds of the respondents indicated that they do not keep their policies up to date on a regular basis.

While you have the responsibility for security policy, you have not had the necessary software support to properly create and implement policies. The NetIQ Security Management products, including VigilEnt Policy Center, provide the only cost-effective way to secure your business by enforcing policy compliance, administering users, minimizing vulnerabilities, and preventing intrusions, to optimize and protect information assets throughout your enterprise.

Industry Terms

VPC uses the following definitions of policy and compliance management terms:

Policy

A policy is a high-level statement of enterprise goals and objectives, accompanied by the reference to all relevant standards. This reference includes the detailed direction for compliance. Policies must be consistent and applicable to the entire organization. This term is often used generically in reference to any of the terms listed in this table, and in some cases, used to identify platform configuration settings.

Standard

A standard is a mandatory activity, action, rule, or regulation that provides the support structure and specific direction that result in meaningful and effective policies. Many standards may relate to one policy.

Procedure

A procedure is the step-by-step process required for the implementation of the requirements set by standards. These procedures can vary by department or business unit.

Guideline

Guidelines are closely related to standards or procedures, but are typically phrased as "should" instead of "must" and the guidance is often interpreted as a suggestion or ignored. As a result, guidelines are ineffective in a corporate governance program.

Best Practice

Use of this term varies widely. For technical people, this term generally refers to a set of instructions or procedures used to secure a particular platform. For business people, this term usually refers to a generally accepted set of policies for their industry, country, or global perception. VPC uses the term, "Leading Practices" to identify policy statement libraries. These libraries contain statements that offer multiple effective options for a single practice, none of which can be singled out as being the "best."

What Is VigilEnt Policy Center?

VPC is the most complete solution for developing, implementing, managing, tracking, training, and reporting on your corporate policies. You can manage all policy types through VPC including information security, privacy, human resources, health, or safety. VPC helps you create accurate policies, verify that your users read and understand the policies, and run reports that can support your attempt to comply with any internal or external requirements.

Develop Policies

Policy documents define roles and responsibilities and inform employees of security requirements. Properly-written policy documents minimize incident costs and help ensure the consistent implementation of controls across an organization.

VPC sample documents provide a shortcut for developing policies. The VPC Policy Library contains collections of policy statements organized by industry standard or regulation.

VPC makes it easy to create and maintain your policies. Simply archive the existing policy document to store your document in case you need the information in the future. Create a copy from the archived file and make the necessary changes. You do not need to create an entirely new file if the information already exists in a document. VPC makes it just as simple to create, review, and maintain quizzes.

Implement Policies

Implementing a strong policy document is the key to a successful information security effort. VPC provides comprehensive sample policies that are clear enough for a user to understand and implement.

You can create user groups and roles, and then customize your policy coverage by sending each group only those policies dealing with that group specialty. Filtering your documents saves time and money, and helps complete the policy coverage in your organization.

Manage Compliance

Correctly written and implemented, policy documents act as a clear statement of management intentions, reducing potential liability. VPC provides quizzing functionality to verify user understanding of current policy content. Quizzes let you measure user knowledge, and use the results in an audit or during a lawsuit as proof of attempted compliance and due diligence.

You can use quizzes to support your implemented policy documents. VPC includes numerous quizzes covering CISSP certification, ISO 17799 assessment, Sarbanes-Oxley awareness, and ISPME policies. Use the related policy statements and quiz questions when creating your documents and you can create a comprehensive, thorough information security solution.

In addition to quizzes, VPC provides a number of reports that give you a snapshot of your policy compliance at any point in time. VPC offers the following reporting topics:

Policy Reports

Let you see results for a single policy document. Run compliance reports to view all of your users who read and accept the policy document, and then run exception reports to view who has not yet complied with your information security compliance effort.

Quiz Reports

Let you see results for a single quiz. Run compliance reports to view all of your users who have completed the quiz along with their scores, and then run exception reports to view who has not yet completed a quiz.

User Reports

Let you see results for a single user or group of users. Run compliance reports to view what documents your selected users read or complete, and then you can run exception reports and view any remaining policy documents or quizzes.

How VigilEnt Policy Center Works

VigilEnt Policy Center has the following three 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.

How Customers Use VigilEnt Policy Center

You can use VPC to provide a centralized policy and compliance management solution in your heterogeneous environment. The following stories show how some of our customers have put VPC to work.

Plan Provider Centralizes Policy Compliance

A leading managed behavioral health company began to address policy awareness as the cornerstone in a total information security solution. VPC helped them simplify the process of creating, reviewing, and implementing vital security and privacy policies at the same time as solving the dilemma of disseminating the information to all offices at once.

The quizzing and reporting features within VPC let the policy group send out online testing to assess and track user awareness of current policy within the organization.

Result: VPC helped an organization centralize and simplify the entire policy creation process in regard to security measures, policies, and procedures. In addition to saving money, time, and resources, VPC helped the company meet HIPAA regulations and key certification requirements such as ISO 9000.

Retailer Saves Money and Time in Document Distribution

A large retail organization needed to update and implement a document concerning new benefits in a 401k. They needed to distribute the document to the entire organization and receive notification from every employee that the document was received, understood, and acknowledged as approved and binding. They contacted the VPC administrator within their organization and inquired as to the availability of VPC to accommodate its needs.

Once distributed, employees read and acknowledged the document, allowing the organization to track, in real time, how successful they were in rolling out the new document.

Result: In addition to drastically reducing the time necessary to distribute the document, VPC helped the company save $30,000 by eliminating the need for printing, administering mail outs, processing returns, and the necessary manpower and postage costs.

Healthcare Organization Achieves Service Excellence

An Australian health service and major specialist referral center had no means of measuring whether staff was reading and comprehending the organization's numerous policies and procedures. It required a user-friendly solution that would encourage and foster the policy understanding and compliance for the 1,000+ staff members located in five companies across four physical locations.

Result: VPC provided centralized, online computer access using a simple Web-based interface accessible from all locations. The organization can accurately measure policy compliance in real-time by ensuring that all users read the policy documents, completed a quiz on the document contents, and signed off on the documents.

How VigilEnt Policy Center Helps You

VPC delivers policy and compliance management that helps organizations develop high-quality information security policies in a short period of time. By increasing the consistency and centralization of all policies in your organization, you drastically reduce your liability.

Reduces the Time to Develop High-Quality Policies

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

- Basel II—International Convergence of Capital Measurement and Capital Standards
- ISO 17799—Code of Practice for Information Technology Management
- NIST 800-53—National Institute of Standards and Technology
- Sarbanes-Oxley—H.R. 3763 Sarbanes-Oxley Act of 2002
- VISA PCI—Payment Card Industry Data Security Standard

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

You can create VPC documents using a Microsoft Word or HTML interface. These tools can decrease the time needed to add a policy document to VPC by those who are comfortable and familiar with Word and HTML.

Decreases Employee Information Overload

Once you have added or synchronized your users and groups to VPC, and you have created and applied roles, you can distribute information to your users. You can disperse policies, standards, procedures, and guidelines based on a role in the organization.

Increases Policy Consistency and Centralization

Through access controls available on the Administration Site, VPC helps you keep your policies in a centralized location and allows you to control access to your policies. You can create a group of policy document administrators to cover each one of your departments, and give each area the ability to issue policies to their workers or the entire organization through a single mechanism.

Decreases Your Legal Liability

By offering quizzes and accurate reports, VPC helps an organization decrease its legal liability by tracking the signatures of employees who have acknowledged that they have read and understood corporate policies. A single compliance report can show the names of every user who has not acknowledged reading a policy document or completing a quiz.

Provides Measurement Tools

VPC includes metrics to ensure that your policy and awareness efforts are having a meaningful impact on your organization. As part of the reporting feature, VPC allows you to send an automatic electronic mail message that non-compliant users must read a specific policy document or complete a certain quiz by a certain date. These reminders may mean the difference between total compliance by a date dictated in a government regulation, and the risk of penalties for non-compliance.

Chapter 2
What are Web Services?

From Wikipedia (http://en.wikipedia.org/wiki/Web_service), the free encyclopedia

> "...a Web service is "a software system designed to support interoperable Machine to Machine interaction over a network." Web services are frequently just Web APIs that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services.

For our purposes, this definition will suffice in that we intend for this documentation to serve as a supplement or action guide for using VPC web services, not for conveying a foundational knowledge of web service technology. If this is your first endeavor into web services as a technology, we recommend that you preempt the reading of this guide with a deeper investigation into the technology as a whole. Once you have a strong understanding, then return to this guide for instruction as to how to utilize the VPC web services in your environment.

Our intent with the VPC web services is to provide dynamic access to the business logic contained in the core VPC product so that you can customize its delivery to applications and frameworks with which your users are more familiar such as corporate portals and intranets. While we feel the VPC GUI is capable within itself to deliver the value to your employees, we also understand the value of embedding the knowledge and functionality within your already established lines of communication.

Advantages of Web Services

Again the wealth of information and argument available on the advantages of web services to an organization is a study far more reaching than we intend to capture in this guide. However, there are a few advantages that we do want to highlight with respect to how we foresee companies utilizing our services.

The advantages are as follows:

- Pliability - Web services allow you to capture essential business logic and build it directly into the current, working fabric of your organization giving you the ability to bring relevant functionality from disparate products into a single point of access and impact (e.g. Dashboard built on functional items pulled from multiple, non-congruent product lines).
- Portability - Web services allow developers within your company to roll up their sleeves and code custom, functional solutions in languages with which they are familiar. So, if you want to display the required policies for employees in your existing .NET/.ASP based intranet you can do so simply by taking advantage of common protocols and standard means of communicating with web services and not have to pay for custom solutions or wait for a future release of the product itself.

Methods

The introductory VPC web services provide methods related primarily to the querying of policy documents.

The methods described in this document are as follows:

- getPolicyListForUser
- getPolicySearch
- getPolicyListForUserLED
- getPolicySearchLED
- getUsersByManager
- getQuizListForUser
- insIncidentReport

For more information about Web Services, see the Administration Site and click **Administration > Options > Web Services**. Once there, you can link to detailed technical information for the available services and also determine if the services are running as expected.

The VPC web services are cataloged according to the following criteria:

- Web service method
- Web service description
- Input and output parameters
- Examples

Read the remainder of this section to gain a more detailed understanding of the VPC services offering.

Method	getPolicyListForUser
Description	The method retrieves the policies assigned to a given VPC user based on client supplied user names, repository names, privilege scopes (required vs. not required), and status (read vs. not read).
Input Parameters	
userID	VPC user ID to whom the policies must be related.
repository	The repository name to which the user belongs (e.g. Internal Repository). The names provided must be an exact match to the actual repository names.
privilegeScope	RR or NR The privilege assigned to the user in relation to the policy document (i.e. RR for Required to Read or NR for Read but Not Required). This parameter is optional. If the user does not provide the privilege scope, the method returns all the policy documents, both required and not required.
completed	read or unread The status of the document in relation to the particular user. This parameter is optional. If the user does not provide the status of the document, the method returns only the unread policy documents.
returnProperties	0 or 1 Indication as to the intent of the request - Return the custom properties (1) or do not return them (0). This parameter is optional. If the user does not provide it, the properties are not displayed.

returnPrivileges	0 or 1 Indication as to intent of the request - Return the privileges (1) or do not return them (0). This parameter is optional. If the user does not provide it, the privileges will not be displayed.
returnLEDList	0 or 1 Indication as to the intent of the request - Return the LED list (1) or not return it (0). This parameter is optional. If the user does not provide it, the LED list will not be displayed.
activeOnly	0 or 1 Indication as to the intent of the request - Return only the non-expired (1) or return all privileged policies (0). This parameter is required and NetIQ Corporation recommends enabling (1) this parameter.
Output Parameters	
title	The title of a policy document.
url	The hyperlink for viewing the policy on the VPC User Site.
availableFrom	yyyy-mm-dd hh:mm:ss.fff The Available From date of the policy document.
availableTo	yyyy-mm-dd hh:mm:ss.fff The Available To date of the policy document.
readDate	yyyy-mm-dd hh:mm:ss.fff The date marking the event of a user having read a policy.
privileges	High-level category specification, its subcategory will be privilege.
privilege	RR which represents Required to Read NR which represents Read but Not Required The privilege assigned to the user in the policy document.
properties	High-level category specification, its subcategory will be a specific property.
property	Subcategory under properties tag, its subcategories will be name and value.
name	The name of a custom property.
value	The value of a custom property.
leds	High-level category specification for list of language-equivalent copies.
led	Subcategory specification for language-equivalent copies of policies. Its subcategories are url, title, and language.
url	The hyperlink for viewing the LED policy on the VPC User Site.
title	The title of an LED policy document.
language	The language of the LED policy document.

Example	
Method Invocation	This example requests all policies for a specified user according to the following parameters: userID = emilyA repository = Internal Repository privilegeScope = RR completed = unread returnProperties = 1 returnPrivileges = 1 returnLEDList = 1 activeOnly = 1 http://vpcserver:8080/Axis2/services/VPCWebServicePack1/getPolicyListForUser?userID=emilyA&repository=Internal%20Repository&privilegeScope=RR&completed=unread&returnProperties=1&returnPrivileges=1&returnLEDList=1&activeOnly=1 This method call employs Security Level 1, anonymous connection capabilities. For more information about security levels, see "Securing Web Services."
XML-based response	- <ns0:getPolicyListForUserResponse xmlns:ns0="http://webservices.netiq.com"> <ns0:authentication_ok>Successfully anonymously logged in</ns0:authentication_ok> - <ns0:policyList> - <ns0:policy> <ns0:title>Document1</ns0:title> <ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=3407181C-8725-4434-A72E-87A63EDC0E1A</ns0:url> <ns0:availableFrom>2010-02-11 04:00:00.0</ns0:availableFrom> <ns0:availableTo>2011-02-11 04:00:00.0</ns0:availableTo> <ns0:readDate /> - <ns0:privileges> <ns0:privilege>RR</ns0:privilege> </ns0:privileges> - <ns0:properties> - <ns0:property> <ns0:name>Country</ns0:name> <ns0:value> USA </ns0:value> </ns0:property> </ns0:properties> - <ns0:leds> - <ns0:led> <ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=3407181C-8725-4434-A72E-87A63EDC0E1A</ns0:url> <ns0:title>Document1</ns0:title> <ns0:language>English</ns0:languageName> </ns0:led>

Method	getPolicySearch
Description	The method searches the available policies of a given user and return a list of available (accessible) policies based on supplied search criteria (Available To/ From dates, text that match title, keyword or full text searching for supported formats or value of custom properties). Note: The search text input supports English-only searches. Multi-language support will be considered in future releases in conjunction with a review of existing site search capabilities.
Input Parameters	
text	The search text.
userID	VPC user ID to whom the policies must be related.
repository	The repository name to which the user belongs (e.g. Internal Repository). The names provided must be an exact match to the actual repository names.
dateFrom	yyyy-mm-dd Starting date for the targeted availability interval.
dateTo	yyyy-mm-dd End date for the targeted availability interval.
returnProperties	0 or 1 Indication as to the intent of the request - Return the custom properties (1) or do not return them (0). This parameter is optional. If the user does not provide it, the properties are not displayed.
returnPrivileges	0 or 1 Indication as to intent of the request - Return the privileges (1) or do not return them (0). This parameter is optional. If the user does not provide it, the privileges will not be displayed.
returnLEDList	0 or 1 Indication as to the intent of the request - Return the LED list (1) or not return it (0). This parameter is optional. If the user does not provide it, the LED list will not be displayed.
activeOnly	0 or 1 Indication as to the intent of the request - Return only the non-expired (1) or return all privileged policies (0). This parameter is required and NetIQ Corporation recommends enabling (1) this parameter.
Output Parameters	
title	The title of a policy document.
url	The hyperlink for viewing the policy on the VPC User Site.
availableFrom	yyyy-mm-dd hh:mm:ss.fff The Available From date of the policy document.
availableTo	yyyy-mm-dd hh:mm:ss.fff The Available To date of the policy document.
properties	High-level category specification. Its subcategory will be a specific property.
property	Subcategory under properties tag. Its subcategories will be name and value.
name	The name of a custom property.
value	The value of a custom property.
privileges	High-level category specification. Its subcategory will be privilege.

privilege	RR which represents Required to Read NR which represents Read but Not Required The privilege assigned to the user in the policy document.
leds	High-level category specification for list of language-equivalent copies.
led	Subcategory specification for language-equivalent copies of policies. Its subcategories will be url, title, and language.
url	The hyperlink for viewing the LED policy on the VPC User Site.
title	The title of an LED policy document.
language	The language of the LED policy document.
Example	
Method Invocation	This example executes a search of the available policy documents based on the following: text = compliance userID = emilyA repository = Internal Repository dateFrom = 2006-01-10 dateTo = 2011-01-01 returnProperties = 1 returnPrivileges = 1 returnLEDList = 1 activeOnly = 1 http://vpcserver:8080/Axis2/services/VPCWebServicePack1/getPolicySearch?credentials=admin/control&text=compliance&userID=emilyA&repository=Internal%20Repository&dateFrom=2006-01-10&dateTo=2009-01-01&returnProperties=1&returnPrivileges=1&returnLEDList=1&activeOnly=1 This method call employs Security Level 2, the inclusion of clear text connection credentials. For more information about security levels, see "Securing Web Services."

XML-based response	- <ns0:getPolicySearchResponse xmlns:ns0="http://webservices.netiq.com"> <ns0:authentication_ok>Successfully anonymously logged in </ns0:authentication_ok> - <ns0:policyListSearch> - <ns0:policySearch> <ns0:title>policy 1</ns0:title> <ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=1C88A5D8-BB3A-42B7-95E9-823169AD607D</ns0:url> <ns0:availableFrom>2009-10-28 04:00:00.0</ns0:availableFrom> <ns0:availableTo>2010-10-28 04:00:00.0</ns0:availableTo> - <ns0:properties> - <ns0:property> <ns0:name>Country</ns0:name> <ns0:value> USA </ns0:value> </ns0:property> </ns0:properties> - <ns0:privileges> <ns0:privilege>RR</ns0:privilege> </ns0:privileges> - <ns0:leds> - <ns0:led> <ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=1C88A5D8-BB3A-42B7-95E9-823169AD607D</ns0:url> <ns0:title>policy 1</ns0:title> <ns0:language>English</ns0:language> </ns0:led> - <ns0:led>
	<ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=04B28BBB-D771-44DD-9918-EE8FFA89A176</ns0:url> <ns0:title>politica 1</ns0:title> <ns0:language>Spanish</ns0:language> </ns0:led> </ns0:leds> </ns0:policySearch> </ns0:policyListSearch> </ns0:getPolicySearchResponse>

Method	getPolicyListForUserLED
Description	The method retrieves the policies assigned to a given VPC user based on client supplied languages, user names, repository names, privilege scopes (required vs. not required), completion status (read vs. not read), and the requirement to return single or multiple language links to the policies.
Input Parameters	
language	Language in which the policy is needed. The expected format for the language identification is the English spelling of the desired, supported language.
userID	VPC user ID to whom the policies must be related.

repository	The repository name to which the user belongs (e.g. Internal Repository). The names provided must be an exact match to the actual repository names.
privilegeScope	RR or NR The privilege assigned to the user in relation to the policy document (i.e. RR for Required to Read or NR for Read but Not Required). This parameter is optional. If the user does not provide the privilege scope, the method will return all the policy documents, both required and not required.
completed	read or unread The status of the document in relation to the particular user. This parameter is optional. If the user does not provide the status of the document, the method will return only the unread policy documents.
returnLangPlusMaster	0 or 1 Indication as to the intent of the request - Return the language equivalent copy of the policy link (0) or return both the LED copy link and the default parent/ master copy link (English) (1). This parameter is optional. If the user does not provide it, the default parent/master copy will not be displayed.
returnProperties	0 or 1 Indication as to the intent of the request - Return the custom properties (1) or do not return them (0). This parameter is optional. If the user does not provide it, the properties will not be displayed.
returnPrivileges	0 or 1 Indication as to intent of the request - Return the privileges (1) or do not return them (0). This parameter is optional. If the user does not provide it, the privileges will not be displayed.
activeOnly	0 or 1 Indication as to the intent of the request - Return only the non-expired (1) or return all privileged policies (0). This parameter is required and NetIQ Corporation recommends enabling (1) this parameter.
Output Parameters	
led	High-level category specification for language-equivalent copies of policies. Its subcategories will be title, language, and URL.
url	The hyperlink for viewing the LED policy on the VPC User Site.
title	The title of the LED policy document.
language	The language of the LED policy document.
master	High-level category specification for the master policy. Its subcategories will be title, language, and URL.
url	The hyperlink for viewing the master policy document on the VPC User Site.
title	The title of the master policy document.
language	The language of the master policy document.
properties	High-level category specification. Its subcategory will be a specific property.
property	Subcategory under the properties tag. Its subcategories will be name and value.
name	The name of a custom property.
value	The value of a custom property.
privileges	High-level category specification. Its subcategory will be privilege
privilege	RR which represents Required to Read NR which represents Read but Not Required The privilege assigned to the user in the policy document.
availableFrom	yyyy-mm-dd hh:mm:ss.fff The Available From date of the policy document.

availableTo	yyyy-mm-dd hh:mm:ss.fff The Available To date of the policy document.
readDate	yyyy-mm-dd hh:mm:ss.fff The date marking the event of a user having read a policy.
Example	
Method Invocation	This example executes a search of the available policy documents based on the following: language = Spanish userID = emilyA repository = Internal Repository privilegeScope = RR completed = unread returnLangPlusMaster = 1 returnProperties = 1 returnPrivileges = 1 activeOnly = 1 http://vpcserver:8080/Axis2/services/VPCWebServicePack1/getPolicyListForUserLED?credentials=admin/control&language=Spanish&userID=emilyA&repository=Internal%20Repository&privilegeScope=RR&completed=unread&returnLangPlusMaster=1&returnProperties=1&returnPrivileges=1&activeOnly=1 This method call employs Security Level 2, the inclusion of clear text connection credentials. For more information about security levels, see "Securing Web Services."

XML-based Response	- <ns0:getPolicyListForUserLEDResponse xmlns:ns0="http:// webservices.netiq.com"> <ns0:authentication_ok>Successfully anonymously logged in </ns0:authentication_ok> - <ns0:policyListLED> - <ns0:policyLED> - <ns0:led> <ns0:url>http:// vpcserver:8080/policy/launch.jsp?cmd=04B28BBB-D771-44DD-9918-EE8FFA89A176</ns0:url> <ns0:title>policy publish 5.5 SP</ns0:title> <ns0:language>Spanish</ns0:language> </ns0:led> - <ns0:master> <ns0:url>http:// vpcserver:8080/policy/launch.jsp?cmd=1C88A5D8-BB3A-42B7-95E9-823169AD607D</ns0:url> <ns0:title>policy publish 5.5</ns0:title> <ns0:language>English</ns0:language> </ns0:master> - <ns0:properties> - <ns0:property> <ns0:name>Country</ns0:name> <ns0:value> USA </ns0:value> </ns0:property> </ns0:properties>
	- <ns0:privileges> <ns0:privilege>RR</ns0:privilege> </ns0:privileges> <ns0:availableFrom>2009-10-28 04:00:00.0</ns0:availableFrom> <ns0:availableTo>2010-10-28 04:00:00.0</ns0:availableTo> <ns0:readDate /> </ns0:policyLED> </ns0:policyListLED> </ns0:getPolicyListForUserLEDResponse>

Method	getPolicySearchLED
Description	The method searches the available policies of a given user and returns a list of available (accessible) policies based on supplied search criteria factoring in the language preference for the results to be returned (Available To/From dates, language, text that match title, keyword, or full text searching for supported formats or value of custom properties) Note: The search text input supports English-only searches. Multi-language support will be considered in future releases in conjunction with a review of existing site search capabilities.
Input Parameters	
text	The search text.
userID	VPC user ID to whom the policies must be related.
repository	The repository name to which the user belongs (e.g. Internal Repository). The names provided must be an exact match to the actual repository names.

dateFrom	yyyy-mm-dd Starting date for the targeted availability interval.
dateTo	yyyy-mm-dd End date for the targeted availability interval.
language	Language in which the policy is needed. The expected format for the language identification is the English spelling of the desired, supported language.
returnLangPlusMaster	0 or 1 Indication as to the intent of the request - Return the language equivalent copy of the policy link (0) or return both the LED copy link and the default parent/ master copy link (English) (1). This parameter is optional. If the user does not provide it, the default parent/master copy will not be displayed.
returnProperties	0 or 1 Indication as to the intent of the request - Return the custom properties (1) or do not return them (0). This parameter is optional. If the user does not provide it, the properties will not be displayed.
returnPrivileges	0 or 1 Indication as to intent of the request - Return the privileges (1) or do not return them (0). This parameter is optional. If the user does not provide it, the privileges will not be displayed.
activeOnly	0 or 1 Indication as to the intent of the request - Return only the non-expired (1) or return all privileged policies (0). This parameter is required and NetIQ Corporation recommends enabling (1) this parameter.
Output Parameters	
led	High-level category specification for language equivalent copies of policies. Its sub-categories are title, language, and URL.
url	The hyperlink for viewing the LED policy on the VPC User Site.
title	The title of an LED policy document.
language	The language of the LED policy document. The expected format for the language identification is the English spelling of the desired, supported language.
master	High-level category specification for the master policy. Its subcategories are title, language, and URL.
url	The hyperlink for viewing the master policy document on the VPC User Site.
title	The title of a policy document.
language	The language of the master policy document.
properties	High-level category specification. Its subcategory is a specific property.
property	Subcategory under the properties tag. Its subcategories are name and value.
name	The name of a custom property.
value	The value of a custom property.
privileges	High-level category specification, its subcategory will be privilege
privilege	RR which represents Required to Read NR which represents Read but Not Required The privilege assigned to the user in the policy document.
availableFrom	yyyy-mm-dd hh:mm:ss.fff The Available From date of the policy document.
availableTo	yyyy-mm-dd hh:mm:ss.fff The Available To date of the policy document.

Example	
Method Invocation	This example executes a search of the available policy documents based on the following: text = compliance userID = emilyA repository = Internal Repository dateFrom = 2006-01-10 dateTo = 2011-01-01 language = Spanish returnLangPlusMaster = 1 returnProperties = 1 returnPrivileges = 1 activeOnly = 1 http://vpcserver:8080/Axis2/services/VPCWebServicePack1/getPolicySearchLED?credentials=admin/control&text=compliance&userID=emilyA&repository=Internal%20Repository&dateFrom=2006-01-10&dateTo=2009-01-01&language=Spanish&returnLangPlusMaster=1&returnProperties=1&returnPrivileges=1&activeOnly=1 This method call employs Security Level 2, the inclusion of clear text connection credentials. For more information about security levels, see "Securing Web Services."

XML-based Response	- <ns0:getPolicySearchLEDResponse xmlns:ns0="http://webservices.netiq.com"> <ns0:authentication_ok>Successfully anonymously logged in</ns0:authentication_ok> - <ns0:policyListSearchLED> - <ns0:policySearchLED> - <ns0:led> <ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=04B28BBB-D771-44DD-9918-EE8FFA89A176</ns0:url> <ns0:title>policy publish 5.5 SP</ns0:title> <ns0:language>Spanish</ns0:language> </ns0:led> - <ns0:master> <ns0:url>http://vpcserver:8080/policy/launch.jsp?cmd=1C88A5D8-BB3A-42B7-95E9-823169AD607D</ns0:url> <ns0:title>policy publish 5.5</ns0:title> <ns0:language>English</ns0:language> </ns0:master> - <ns0:properties> - <ns0:property> <ns0:name>Country</ns0:name> <ns0:value>USA</ns0:value> </ns0:property> </ns0:properties>
	- <ns0:privileges> <ns0:privilege>RR</ns0:privilege> </ns0:privileges> <ns0:availableFrom>2009-10-28 04:00:00.0</ns0:availableFrom> <ns0:availableTo>2010-10-28 04:00:00.0</ns0:availableTo> </ns0:policySearchLED> </ns0:policyListSearchLED> </ns0:getPolicySearchLEDResponse>

Method	getUsersByManager
Description	The method retrieves the users that have been assigned to a given user as a manager based on client-supplied user name and repository name.
Input Parameters	
manager	VPC user ID of the manager responsible for the users.
repository	The repository name to which the user belongs (for example, Internal Repository). The names provided must be an exact match to the actual repository names.
Output Parameters	
userID	VPC user ID of the user who has as a manager the user used in the web service call.
firstName	The first name of the user.
lastName	The last name of the user.
repository	The repository to which the user belongs.

Example	
Method Invocation	This example requests all the users that have as a manager the specified user according to the following parameters: manager = emilyA repository = Internal Repository http://vpcserver:8080/Axis2/services/VPCWebServicePack1/getUsersByManager?manager=emilyA&repository=Internal%20Repository This method call employs Security Level 1, anonymous connection capabilities. For more information about security levels, see "Securing Web Services."
XML-Based Response	-<ns0:getUsersByManagerResponse xmlns:ns0="http://webservices.netiq.com"> <ns0:authentication_ok>Successfully logged in</ns0:authentication_ok> -<ns0:userList> -<ns0:user> <ns0:userID>maria.claros</ns0:userID> <ns0:firstName>Maria</ns0:firstname> <ns0:lastName>Claros</ns0:lastname> <ns0:repository>Internal Repository</ns0:repository> </ns0:user> -<ns0:user> <ns0:userID>berreth.rodney</ns0:userID> <ns0:firstName>BERRETH</ns0:firstname> <ns0:lastName>RODNEY</ns0:lastname> <ns0:repository> Internal Repository </ns0:repository> </ns0:user> </ns0:userList> </ns0:getUsersByManagerResponse>

Method	getQuizListForUser
Description	The method retrieves the quizzes assigned to a given VPC user based on client-supplied user names, repository names, privilege scopes (required vs. not required), and status (read vs. not read).
Input Parameters	
userID	VPC user ID to whom the quizzes must be related.
repository	The repository name to which the user belongs (e.g. Internal Repository). The names provided must be an exact match to the actual repository names.
privilegeScope	RR or NR The privilege assigned to the user in relation to the quiz document (i.e. RR for Required to Read or NR for Read but Not Required). This parameter is optional. If the user does not provide the privilege scope, the method returns all the quiz documents, both required and not required.
completed	Read, unread, or all The status of the document in relation to the particular user. This parameter is optional. If the user does not provide the status of the document, the method returns only the unread quiz documents.

returnProperties	0 or 1 Indication as to the intent of the request - Return the custom properties (1) or do not return them (0). This parameter is optional. If the user does not provide it, the properties are not displayed.
returnPrivileges	0 or 1 Indication as to intent of the request - Return the privileges (1) or do not return them (0). This parameter is optional. If the user does not provide it, the privileges will not be displayed.
activeOnly	0 or 1 Indication as to the intent of the request - Return only the nonexpired (1) or return all privileged quizzes (0). This parameter is required and NetIQ Corporation recommends enabling (1) this parameter.
Output Parameters	
title	The title of a quiz document.
url	The hyperlink for viewing the quiz on the VPC User Site.
availableFrom	yyyy-mm-dd hh:mm:ss.fff The Available From date of the quiz document.
availableTo	yyyy-mm-dd hh:mm:ss.fff The Available To date of the quiz document.
submitted	yyyy-mm-dd hh:mm:ss.fff The date marking the event of a user having read a quiz.
score	The latest score for a given quiz.
privileges	High-level category specification. Its subcategory is privilege.
privilege	RR which represents Required to Read NR which represents Read but Not Required The privilege assigned to the user in the quiz document.
properties	High-level category specification. Its subcategory is a specific property.
property	Subcategory under properties tag. Its subcategories are name and value.
name	The name of a custom property.
value	The value of a custom property.
Example	
Method Invocation	This example requests all quizzes for a specified user according to the following parameters: userID = emilyA repository = Internal Repository privilegeScope = RR completed = read returnProperties = 1 returnPrivileges = 1 activeOnly = 1 http://vpcserver:8080/Axis2/services/VPCWebServicePack1/getQuizListForUser?userID=emilyA&repository=Internal%20Repository&privilegeScope=RR&completed=read&returnProperties=1&returnPrivileges=1&activeOnly=1 This method call employs Security Level 1, anonymous connection capabilities. For more information about security levels, see “Securing Web Services” on page 25.

XML-Based Response	<ns0:getQuizListForUserResponse xmlns:ns0="http:// webservices.netiq.com"> <ns0:authentication_ok>Successfully anonymously logged in </ns0:authentication_ok> <ns0:quizList> <ns0:quiz> <ns0:title>quizMe</ns0:title> <ns0:url>http://vpcserver:8080/policy/
	launch.jsp?cmd=D3846003-832C-4933-A7BF-CCD82FA67085</ns0:url> <ns0:availableFrom>2010-11-26 04:00:00.0</ns0:availableFrom> <ns0:availableTo>2010-12-26 04:00:00.0</ns0:availableTo> <ns0:submitted>2010-11-26 16:53:33.907</ns0:submitted> <ns0:score>33</ns0:score> <ns0:privileges> <ns0:privilege>RR</ns0:privilege> </ns0:privileges> <ns0:properties> <ns0:property> <ns0:name>Country</ns0:name> <ns0:value>USA</ns0:VALUE> </ns0:property> </ns0:properties> </ns0:quiz> </ns0:quizList> </ns0:getQuizListForUserResponse>

Method	insIncidentReport
Description	The method is used to report incidents related to policy violations, erroneous activities, or any type of incident defined previously.
Input Parameters	
Uid	User ID The VPC user ID to whom the incident report must be related. If the user ID should be anonymous, you can enter `anonymous` in the Uid field, enter a user ID not related to the repository, or leave the field blank. The fields IT (Type of Incident) and Des (Brief Description) are required fields and must be entered whether the report is anonymous or not.
R	Repository The name of the repository to which the user belongs (e.g., Internal Repository). The name provided must be an exact match to the actual repository name. Otherwise, the incident report will be sent as anonymous (if anonymous incident reporting has been enabled).
RN	Name The name of the contact to whom the incident report must be related.
RP	Phone Number The phone number of the contact to whom the incident report must be related.
RF	Fax The fax number of the contact to whom the incident report must be related.

RE	E-mail The email address of the contact to whom the incident report must be related.
SN	Name of System The name of the affected system.
SIP	IP Address of System The IP address of the affected system.
SOS	OS Type/Version The operating system type/version of the affected system.
SH	Hardware Manufacturer The hardware manufacturer of the affected system.
SS	Serial Number The serial number of the affected system.
SP	Corporate Property Number The corporate property number of the affected system.
iNC	System Connected to Network 0 or 1 Indicates whether the system is connected to a network. If not provided, the default value will be 0.
iMC	System Connected to Modem 0 or 1 Indicates whether the system is connected to a modem. If not provided, the default value will be 0.
LA	Address The address of the area where the incident occurred.
LR	Room The room where the incident occurred.
LB	Building The name of the building where the incident occurred.
DDT	Date/Time Details The date and time when the incident occurred. If known, it should be stated.
DLI	Location of Incident Indicates where the incident occurred (e.g., the store, distribution center number, or department).
DA	Additional Contacts Information The names and contact information of other persons, if any, who may have knowledge of this incident.
IT	Type of Incident Indicates which type of incident occurred. The type of incident provided must be an exact match to the type of incidents registered. If the incident report is anonymous, the type of incident must be available for that task. IT (Type of Incident) is a required field.
Des	Brief Description A short description about what kind of incident happened. This field should be set. Des (Brief Description) is a required field.

Output Parameters	VPC displays two types of messages, depending on whether or not the incident report was submitted anonymously. In the following example, the incident report was submitted by an identifiable person (i.e., not anonymously): <ns0:incidenstring>Your incident report has been submitted. The tracking number for the incident is IR_20110120_1.</ ns0:incidenstring> (Note: The IR_number will vary.) In the following example, the incident report was submitted anonymously: <ns0:incidenstring>Your incident report has been submitted. </ ns0:incidenstring>
Example	
Method Invocation	This example reports an incident according to the following parameters: Uid = emilyA R = Internal Repository RN = Emily Anderson RP = RF = RE = SN = SIP = SOS = SH = SS = SP = iNC = iMC = LA = LR = LB = DDT = DLI = DA = IT = Hoax Des = description http://vpcserver:8080/Axis2/services/VPCWebServicePack1/insIncidentReport?Uid=emilyA&R=Internal%20Repository&RN=Emily%20Anderson&RP=&RF=&RE=&SN=&SIP=&SOS=&SH=&SS=&SP=&iNC=&iMC=&LA=&LR=&LB=&DDT=&DA=&IT=Hoax&Des=description This method call employs Security Level 1, anonymous connection capabilities. For more information about security levels, see “Securing Web Services” on page 25.
XML-Based Response	<ns0:insIncidentReportResponse xmlns:ns0="http:// webservices.netiq.com"> <ns0:authentication_ok>Successfully anonymously logged in </ns0:authentication_ok> <ns0:incidenstring>Your incident report has been submitted. The tracking number for the incident is IR_20110120_1.</ ns0:incidenstring> </ns0:insIncidentReportResponse>

You have been presented with the web service knowledge of all the offered services within VPC. Before you begin to implement the services, we recommend you first study the associated levels of security.

Securing Web Services

The following guidance is provided to help ensure the security of VPC Web Services when implemented within an organization. The recommendations should be considered as an adjunct to your own security practices and not necessarily be the sole means of security.

Implemented Web Services have four security levels:

- No credentials
- Clear-text credentials
- Packed credentials
- Packed credentials with client IP restriction

The following descriptions are provided to inform the use of the services with respect to the various security levels:

Level 1: No credentials

The availability and use of the services are not restricted for any users.

Level 2: Clear-text credentials

The availability and use of the services require user login and password, but no encryption will be used in their transmission. If the user credentials are not valid the web services will not work.

Level 3: Packed credentials

The availability and use of the services can be restricted to designated users who have been given explicit access rights. For example, you can grant access to a user or group of users, create an encrypted packet for access and then deliver it to the targeted users. This will serve as a verification parameter before access to the web service is granted in that if the packet is not validated, the web services will not work.

Level 4: Packed credentials with client IP restriction

The availability and use of the services can be restricted to a specific user and IP address. For example, you can grant access to a specified user, create an encrypted packet for access, and assign the valid IP address to the packet. If the packet is used with a different IP address the web services will not work.

Once you have decided on an appropriate level of security, continue to the next section.

Creating Credentials

Credentials allow you to ensure that the user attempting to invoke the service is permissioned to do so. You can control the breadth of service use simply by limiting the number of people with access to the credential creation and validation process.

When creating credentials, you will need to have a basic understanding of the parameters involved in the transaction.

Parameters	Description
Repository Name	The VPC repository in which the user invoking the services exists.
User Login Name	The VPC User ID for the user attempting to invoke the services.
User Password	The VPC password for the user attempting to invoke the services.
IP Restriction	The IP address or range of addresses that will serve as the valid range from which services can be invoked.

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 create security credentials:

1. Open a command prompt and navigate to the following folder on the VPC server:

   `install_folder``\bin\`

2. Run the following command:

   `credentialsGenerator.bat`

3. When prompted, enter the following parameters: Repository Name, User Login Name, User Password, and IP Restriction.

   This will create a credentials string that is saved in the following location:
   `install_folder``\`*`server`*`\credentials.txt`

Once you have created the credentials, proceed to the next section.

Validating Security

In an effort to provide consumers with the ability to validate the security of the given web services, this section offers guidance as to how to use verify security levels through the use of a provided web service.

Note
The use of *`vpcserver`* in the service URLs may need to be modified to match the server on which you are attempting to make the request.

The web service used to test security is VPCWebServiceDyn. The method used is HelloWorld. The service is available through the following URL:
`http://`*`vpcserver`*`:8080/Axis2/services/VPCWebServiceDyn?wsdl`

Notes
You need access to the VigilEnt Policy Center database to complete the tasks.

You will need to log on to the VPC Administration Site with appropriate permissions for configuring web services. Access to the Web Services tab is limited to users with the Configure VPC Web Services permission. For more information about permissions, see the *VigilEnt Policy Center User Guide*.

To configure Security Level 1 for web service connections:

1. Log on to the VPC Administration web site.
2. On the Administration tab, click **Options**, and then click **Web Services**.
3. Select security level 1 from the available options.
4. Click **Update** to save the security setting.
5. Open a command prompt, and enter the following address:

   ```
   http://vpcserver:8080/Axis2/services/VPCWebServiceDyn/HelloWorld
   ```

   The following message should appear confirming the basic authentication:

   ```
   <ns0:authentication_ok>Successfully anonymously logged in
   </ns0:authentication_ok>
   ```

   You can now see the result of the HelloWorld method:

   ```
   <ns:return>
   This is the VPC Web Service running at: lvf-wk3-dev. It is running on Microsoft
   SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-
   2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: ) .
   The VPC version is: 2. Server time: Fri Nov 16 18:34:58 GMT-04:00 2007.
   </ns:return>
   ```

To configure Security Level 2 for web service connections:

1. Log on to the VPC Administration web site.
2. On the Administration tab, click **Options**, and then click **Web Services**.
3. Select security level 2 from the available options. Proceed with the determination of the connection accounts.
4. 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**.
5. Click **Search**.
6. Select the users or groups you want to enable as connection accounts, and then click **>>** to move them to the Selected Users/Groups box.
7. Click **Update**.
8. Open a command prompt, and enter the following address:

   ```
   http://vpcserver:8080/Axis2/services/VPCWebServiceDyn/
   HelloWorld?credentials=username/password
   ```

   where *username* is a valid user logon name and *password* is the matching password.

Note

At least one of the selected users/groups for targeted connection accounts must match the username/password specified in the connection URL.

One of the following messages should appear confirming the success of the actions taken:

- If no credentials were added:

```
<ns0:authentication_error>User/Password not supplied.
</ns0:authentication_error>
```

- If wrong credentials were added:

```
<ns0:authentication_error>Wrong user/password.
</ns0:authentication_error>
```

- If correct credentials were added:

```
<ns0:authentication_ok>Successfully logged in
</ns0:authentication_ok>
```

If the login is successful, you will be able to see the result of the HelloWorld method:

```
<ns:return>
This is the VPC Web Service running at: lvf-wk3-dev. It is running on Microsoft
SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-
2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: ) .
The VPC version is: 2. Server time: Fri Nov 16 18:34:58 GMT-04:00 2007.
</ns:return>
```

To configure Security Level 3 for web service connections:

1. Log on to the VPC Administration web site.
2. On the Administration tab, click **Options**, and then click **Web Services**.
3. Select security level 3 from the available options. Proceed with the determination of the connection accounts.
4. 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**.
5. Click **Search**.
6. Select the users or groups you want to enable as connection accounts, and then click **>>** to move them to the Selected Users/Groups box.
7. Click **Update**.
8. Open a command prompt, and enter the following address:

   `http://`*`vpcserver`*`:8080/Axis2/services/VPCWebServiceDyn/HelloWorld?credentials=`*`packedstring`*

   where *`packedstring`* is the credential string created in "Creating Credentials" on page 25.

Note

The selected users/groups for targeted connection accounts must match the users/groups entered when creating the credentials.

One of the following messages should appear confirming the success of the actions taken:

- If a wrong credential string was added:

```
<ns0:authentication_error>Packed credentials corrupted.
</ns0:authentication_error>
```

- If a correct credential string was added:

```
<ns0:authentication_ok>Successfully logged in
</ns0:authentication_ok>
```

If the login is successful, you will be able to see the result of the HelloWorld method:

```
<ns:return>
This is the VPC Web Service running at: lvf-wk3-dev. It is running on Microsoft SQL
Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003
Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: ) . The VPC
version is: 2. Server time: Fri Nov 16 18:34:58 GMT-04:00 2007.
</ns:return>
```

To configure Security Level 4 for web service connections:

1. Log on to the VPC Administration web site.
2. On the Administration tab, click **Options**, and then click **Web Services**.
3. Select security level 4 from the available options. Proceed with the determination of the connection accounts.
4. 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**.
5. Click **Search**.
6. Select the users or groups you want to enable as connection accounts, and then click **>>** to move them to the Selected Users/Groups box.
7. Click **Update**.
8. Open a command prompt, and enter the following address:

   `http://`*`vpcserver`*`:8080/Axis2/services/VPCWebServiceDyn/HelloWorld?credentials=`*`packedstring`*

   where *`packedstring`* is the credential string created in "Creating Credentials" on page 25.

Note
The selected users/groups for targeted connection accounts must match the users/groups entered when creating the credentials.

One of the following messages should appear confirming the success of the actions taken:

- If a wrong credential string was added:

```
<ns0:authentication_error>Packed credentials corrupted.
</ns0:authentication_error>
```

- If a correct credential string was added:

```
<ns0:authentication_ok>Successfully logged in
</ns0:authentication_ok>
```

If the login is successful, you will be able to see the result of the HelloWorld method:

```
<ns:return>
This is the VPC Web Service running at: ServerWin001. It is running on Microsoft SQL
Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003
Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: ) . The VPC
version is: 2. Server time: Fri Nov 16 18:34:58 GMT-04:00 2007.
</ns:return>
```

You have been presented with a comprehensive knowledge of all the available security levels for accessing the VPC web services, with this knowledge you can choose the security level that fits best for your company and begin learning how to implement the offered services within the fabric of your existing organization.

Chapter 3
Usage Guidelines

The most simplistic means of services invocation is through the use of a browser URL. Using standard http protocol you can generate URLs to invoke the service methods and return the desired data.

For example, the following URL could be used to invoke a method to return the required policies for the specified user ("Smithj"):

```
http://vpcserver:8080/Axis2/services/VPCWebServicePack1/
getPolicyListForUser?userID=smithj&repository=repName&privilegeScope=RR&completed=u
nread&returnProperties=1&activeOnly=1
```

Likewise, any of the available methods could be manipulated in this same manner based on their input parameters to return results as specified in the method descriptions. While the use of the URL invocation is straight forward, we recommend that it be used mainly for test purposes.

A more practical and robust methodology for invoking the service is through the use of SOAP protocol specifically designed for exchange of information in a decentralized, distributed environment. The expectation is that developers within each organization will write code using the SOAP specification to invoke the methods, capture the results, and then parse the data with additional code to format it for customized display in company intranets or other specialized end points.

To this end, code snippets in .Java and .NET have been provided and can be used as a model for building the basic request-response structure necessary to interacting with the service. The code samples are available within the VPC installation directory in the following directory:

Installdir/Examples

To ensure optimal results when implementing the web services, ensure you adhere to the following guidance:

- Ensure the input/output parameters are spelled correctly in the invocation code.
- Ensure the required input parameters are represented in the invocation code. Omission of the required parameters will result in the failure of the services.
- Ensure the repository names specified as input directly match the names of the repositories or domains in use. This matching is of critical importance when IIS pass-through authentication is being used.
- Ensure the **Enabled Integrated Windows Authentication** browser setting is disabled. Based on the manner in which VPC integrates with IIS for authentication purposes, this setting must be disabled or users attempting to authenticate will be asked to reenter their credentials.

- Ensure you capture responses consisting of empty result sets in your custom code so you can message appropriately to integrated display screens that no results were found.
- Many of the methods return policy properties as output parameters. If you had added custom properties to your policies, it is feasible that you parse the results of the service request according to those values. Understand that you would need to write the parsing mechanism within your source code (file making the request) but it would allow you to present a more dynamic representation of the data for your users.

Sample 1: Viewing Policies on Intranet

Use Case Description

RH&P is a manufacturing company in the Midwest United States. The company has an intranet portal through which all company communication is channeled. When employees sign onto the portal, they view page content based on their site preferences, access privileges, and roles. When clicking on the Policy Governance tab of the portal, the page displays all policies to which the particular user has access - split in groups across those to which they must comply and those that are for informational purposes only. The policy titles appear on the page as hyperlinks that once accessed by the user spawns a viewing window within which the policy appears for reading and/or acknowledgment.

Web Service Deployment

In this case, the getPolicyListForUser method would be targeted since it retrieves policies assigned to a given VPC user. The source of the request (custom code) would invoke the method and the results for the specified user would be returned. The data could then be parsed by the source to display according to the presence of either the RR or NR VPC document privilege. The policy titles could then be displayed as hyperlinks so that when clicked the specific policy would appear in VPC for sign-off or viewing purposes.

An alternative approach would be to use the getPolicyListForUserLED method. The substitution would allow you to specify the language of the policy you want to view (i.e. Spanish copy of an English Code of Conduct policy). By doing so, intranet pages that offer text in native languages would automatically be able to retrieve titles and text for policies matching that same language or return a default language such as English if an equivalent language specific copy was not found.

Sample 2: Searching Policies from a Portal

Use Case Description

Continuing from Sample 1, a separate section of the Policy Governance pages allows a user to search for corporate policies based on keyword entry or dates of policy availability. Once the search request is submitted, the list of policy results will appear filtered according to the requesting user's access privileges and second for the policies that match the search criteria.

Web Service Deployment

For this approach the getPolicySearch method would be utilized. The source of the request (custom code) would invoke the method and the results for the specified user would be returned assuming there is a match of the keyword to the available policies. The resultant data could then be parsed by the source to display according to the titles of the policies. The policy titles, again displayed as hyperlinks, would open the specific policy in VPC for sign-off or viewing purposes when clicked.

An alternative approach would be to utilize the getPolicySearchLED method. The substitution would again allow you to specify the language of the policy you want to view (i.e. French copy of an English Acceptable Use Internet policy). So if your keyword search criteria found a match, you could specify the copy to be returned as French with a default English version as the backup in case no language specific copy is found.

Expectations for Assistance

The use of VPC Web Services is not for everyone. Most companies do not have the resources or interest in customizing the deployment of VPC simply because the core product meets or exceeds the existing needs of the organization. However, for those companies with questions concerning the value of services, how they might be used, or implementation issues the following directives have been established:

NetIQ Sales Account Representatives

- Discussion of VPC Web Service value proposition
- Demonstration of VPC Web Service (Sales Engineers)

NetIQ Professional Services Engagement (At-Cost)

- Discovery of use calls and inquiries that require scoping or cost estimates
- Assistance/troubleshooting with writing, deploying, or analyzing VPC Web Services in a custom environment
- Problems manipulating data returned from VPC Web Service requests

NetIQ Technical Support

VPC core product issues