Global Information Assurance Certification Paper

Auditing for Policy Compliance with QualysGuard and CIS Benchmarks

GIAC (GSNA) Gold Certification

Author: Stewart James, stewart@stootles.com

Advisor: Rodney Caudle

Accepted: August 10th 2010

Abstract

This paper will guide a user through the creation of Policy Compliance tests within the QualysGuard Policy Compliance module. A focus on the Windows 2008 Centre for Internet Security benchmark will be followed for these tests, though the process and concepts can be applied to any technology supported by the QualysGuard Policy Compliance module. Creation of reporting templates for ongoing reporting of compliance status will be covered. The ability to flag an audit exception as acceptable will be introduced and demonstrated.

1. Introduction

In today's information security world, most enterprises are either already moving toward or seriously considering moving toward compliance with any number of a variety of security standards that represent best practice (SANS, 2010a).

There is always a risk that the efforts to gain compliance with an external body fade after the initial audit is performed. Ongoing reporting and measuring is required to ensure consistent compliance. Once an initial audit it is completed, it is possible for people to focus on other areas of their business, unless there are follow up audits to ensure ongoing compliance, it is quite possible for some items to fall out of compliance. Continual measurement and reporting will aide in raising awareness to any areas that may need addressing.

When considering a toolset for measuring information systems compliance with a standard, ongoing reporting should be a concern. There are good tools available to do the “right now” scanning and reporting. A great tool also allows you to automate ongoing scanning, the subsequent tracking of issues and reporting.

QualysGuard is able to provide in depth reporting and tracking for many individual system settings. This information is presented in a web interface and able to generate individual system reports and/or organisation wide score cards.

1.1. Why Perform Compliance Auditing

There are a number of reasons that compliance auditing may be required. Technology specific standards such as those identified in the Payment Card Industry Data Security Standard provide specific rules for information systems involved with the processing of credit card transfers and related services.

Other regulations and standards are not as specific and require a person to follow a logical path of thought and then apply those to any relevant information systems. This is highlighted in the SANS On Demand LEG 413 lectures in regards to the requirements for Sarbanes Oxley. (SANS, 2010c)

Stewart James stewart@stootles.com

Australia mandates that organisations follow 10 privacy principles. It is technology agnostic yet provides clear guidance on securing private information:

> ***Principle 4 - Storage and security of personal information***
>
> A record-keeper who has possession or control of a record that contains personal information shall ensure:
>
> (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
> (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

(Australian Government, 2008)

There are also a number of National Privacy Principles. A plain English version is available from the Office of the Privacy Commission web site. It simplifies the above statements further:

- An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

(Australian Government)

> Personal information is information that identifies you or could identify you. There are some obvious examples of personal information, such as your name or address. Personal information can also include medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work - basically, any information where you are reasonably identifiable.
>
> Information does not have to include your name to be personal information. For example, in some cases, your date of birth and post code may be enough to identify you.
>
> To be precise, the Privacy Act definition of personal information is:
>
> *"... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."*

(Office of the Privacy Commissioner, B)

Stewart James stewart@stootles.com

The Australian Privacy Commissioner has many resources available to aide an organisation in meeting or exceeding reasonable levels of care for personal information. Consider whether you can achieve your purpose without disclosing personal information (Office of the Privacy Commissioner, A). There are many reasons why an organisation may have previously openly shared personal information. Ensuring the sharing of any information is still required to meet the specified purpose is a positive approach to managing personal information.

Defining what reasonable steps to take in securing personal information varies from system to system and organisation to organisation. Methods might include checking that all personal information has been removed from computers before you sell them, installing firewalls, cookie removers and anti-virus scanners on work IT systems, keeping hard copy files in properly secured cabinets, training staff in privacy procedures and allowing file access to staff on a 'need to know' basis only. (Office of the Privacy Commissioner, A)

Any system that will be processing personal information should undergo a risk assessment. This risk assessment can be used to ensure the organisation is comfortable that all reasonable and viable steps and controls are in place. Stepping aside from the technical matters, key will be user training and awareness. Security is a process, not a product (Schneier, 2000). Ongoing awareness by staff to ensure an organisation is always being reasonable in protecting personal information is required.

If an organisation is able to produce evidence in the form of normal business records (SANS, 2010c) that they have been measuring their information systems via regular compliance auditing and taking any relevant corrective action, they will be in a strong position to challenge any claims that due care has not been followed. This documentation may even circumvent any significant legal or social claims against the organisation.

1.2. What is Compliance Auditing

Auditing systems may be for mandated reasons such as Sarbanes Oxley or Graham Leach Bliley Acts in the USA, Payment Card Industry standards globally for those organisations dealing with credit cards or to ensure compliance with a countries privacy laws. These audits

may also be required as part of a fiscal audit to ensure that all systems involved in financial processing are secured to an appropriate standard.

The most important part of compliance auditing is that a formal decision has been made about the standard configuration to be used within an enterprise. This gives an auditor a bar for which to measure against.

Compliance auditing is simply measuring whether that defined standard configuration is in place for a given system or not. Where a system does not meet the defined standard an audit exception is raised (SANS, 2010b). Where an exception is an acceptable deviation from the standard, some supporting documentation should be gathered and included in any subsequent reports (SANS, 2010b)

1.3. What is the Center for Internet Security

The Center for Internet Security (CIS) is a non-profit enterprise that helps organizations reduce risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS provides enterprises with consensus best practice standards for security configurations, as well as resources for measuring information security status and for making rational decisions about security investments (Center for Internet Security, 2010).

As vendors do not develop the CIS benchmarks, they can be seen as a subjective, independent starting point (SANS, 2010b). The CIS benchmarks are an excellent starting point for an enterprise looking at defining the standard that they expect their systems to meet.

They are also an excellent resource for an auditor when dealing with an enterprise that has not yet decided on such detailed configuration. Researching for an Audit can take a significant amount of time. Each item in the benchmarks from the CIS is fully documented and explained. This means that all the research is already done for you. (SANS, 2010b)

The CIS benchmarks are used in this paper as a reference to ensure time is spent focusing on the “how” of the Qualys compliance scanner rather than “why” a specific setting is being tested.

Stewart James stewart@stootles.com

Administrators may also find the CIS benchmarks engaging as they directly reference any area that has been identified by the CIS community as an issue and allowing administrators' access to this group "think tank".

CIS provides high-level checklists models for a quick audit verification process. They also provide a detailed benchmark that explores why a setting should be altered from the default and the impact of altering the setting. **Error! Reference source not found.**1 includes a sample from the Windows 2008 benchmark, Version 1.0 (Center for Internet Security, 2010).

This paper is relying on the benchmarks provided by the CIS. A company's compliance baseline could and should be derived from their policies, procedures and standards.

1.1.1 Enforce password history

Description:
This control defines the number of unique passwords a user must leverage before a previously used password can be reused. For all profiles, the recommended state for this setting is `24 or more passwords remembered`.

Rationale:
Enforcing a sufficiently long password history will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential. For example, if an attacker compromises a given credential that is then expired, this control prevents the user from reusing that same compromised credential.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account
Policies\Password Policy\Enforce password history
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`24 passwords remembered`

References:
CCE-2237-6

Figure 1 Sample recommendation from CIS benchmark

The benchmarks offer an easy checklist with readily accessible reference points and titles, as in this case "1.1.1" and "Enforce password history" respectively. Where there needs to

be discussions surrounding the suitability of a recommendation, full details are provided. External references are also noted where applicable.

The Windows 2008 Benchmark is nearly 160 pages long. The extensive coverage of CIS recommendations helps ensure the ongoing security of the Windows 2008 platform. The CIS Benchmarks are an excellent starting point for any enterprise wanting to document their preferred configuration.

1.4. Compliance auditing in a large enterprise

A significant challenge with compliance auditing is ensuring the ongoing positive impact on production systems. CIS provides a tool for scanning a single system (SANS, 2010b). This tool requires a person to authenticate to the system, deploy and run the software. The tool is an excellent resource for a small number of scans.

In a large environment, manual operations are a bottleneck that will reduce the raw number of hosts that will be regularly scanned. In some environments, it may even render the ongoing scanning impossible to manage as more important business focused priorities take precedence. Delivering a highly automated compliance-auditing tool to an enterprise will enable it to benefit from ongoing testing, with minimal burden placed on employees to perform the actual tests.

Nessus, while now requiring a fee for full functionality (Tenable Network Security)is able to perform the tests remotely. While this reduces the overhead required to perform the tests, a manual review is required to identify if anything has changed.

The commercial space is offering improved options. Qualys is one of the top performers for vulnerability management (Qualys, 2010a). Compliance management seems to be a natural extension as many vulnerability scanners (Nessus, nCircle and Qualys) offer these services.

Qualys, like others in this arena, simplifies the creation of compliance testing as well as the ongoing scanning and reporting. When scanning several hundred systems, being able to automate any part of compliance auditing saves a significant amount of time. Qualys automates the majority of an ongoing compliance auditing:

- Scanning at regular intervals
- Identifying any issues of non-compliance
- Ignoring issues that are not compliant but deemed acceptable in the past.

Later there will be a demonstration of how once established, ongoing compliance auditing with Qualys has minimal operational overhead, as long as there is nothing out of compliance!

1.5. What is QualysGuard

Qualys' on demand approach to IT security and compliance enables organizations of all sizes to successfully achieve both vulnerability management and policy compliance initiatives cohesively, while reducing costs and streamlining operations. Using an innovative Software as a Service (SaaS) approach, the QualysGuard® Security and Compliance Suite combines Qualys' industry leading vulnerability management service with a comprehensive IT compliance solution (Qualys, 2010b).

QualysGuard offers a number of key features:

- SaaS deployment model.
- The extensive data collected is not stored on your disks
- Zero maintenance of the QualysGuard tool or the internal scanning engines
- The data from Vulnerability Scanning and Policy Compliance Auditing is all stored within the single web interface
- Qualys automatically updates the internal scanning engines with the latest vulnerability signatures.
- Extensive reporting capabilities
- Data is encrypted per customer and is not viewable by anyone outside of that customers account, even by Qualys staff.

A more in depth review of QualysGuard as a Vulnerability Management tool is available in the SANS Reading Room. “Creating a comprehensive Vulnerability Assessment Program for

a Large Company Using QualysGuard" (Proffit, 2008), is an excellent review of the underlying product and how the system is used for Vulnerability Scanning.

1.6. Reminder: Always get Authority to Audit in writing

When performing any sort of audit, be sure you have permission from the system and network owners. The person asking for an audit may not have the authority to grant you permission to perform the audit. If a person using a shared hosting arrangement requests an audit of their web site, you probably also want permission from the web sites hosting service. Even if a dedicated server is used, you need to ensure the company housing the website have given you their blessing. After all, your traffic will be flowing through their network.

Always get the authority to perform an Audit in writing and ensure you have it from the right person. Check any records that are reasonable to ensure that you have the right person or persons giving you the go ahead before you get started (SANS, 2010b).

Not getting the right permissions could bring you legal issues via the true system owner.

1.7. QualysGuard Compliance Auditing Capabilities

Using **QualysGuard® Policy Compliance (PC)** an organization can reduce the risk of internal and external threats, while at the same time provide proof of compliance demanded by auditors across multiple compliance initiatives. QualysGuard PC provides an efficient and automated workflow that allows IT security and compliance professionals to:

- *Define policies* that describe how an organization will provide security and integrity.
- *Provide proof* that the policies have been operationalized.
- *Give documented* evidence that the organization has discovered and fixed any policy compliance lapses.

(Qualys, 2010b)

QualysGuards real strength is the ability to perform ongoing regular audits with almost no effort after initial configuration. The QualysGuard system also alerts administrators and auditors of any issues that need to be addressed and can record any explanations of ongoing non-compliance through the notion of "exceptions". The reporting system allows for detailed documents as well as high-level scorecards.

Stewart James stewart@stootles.com

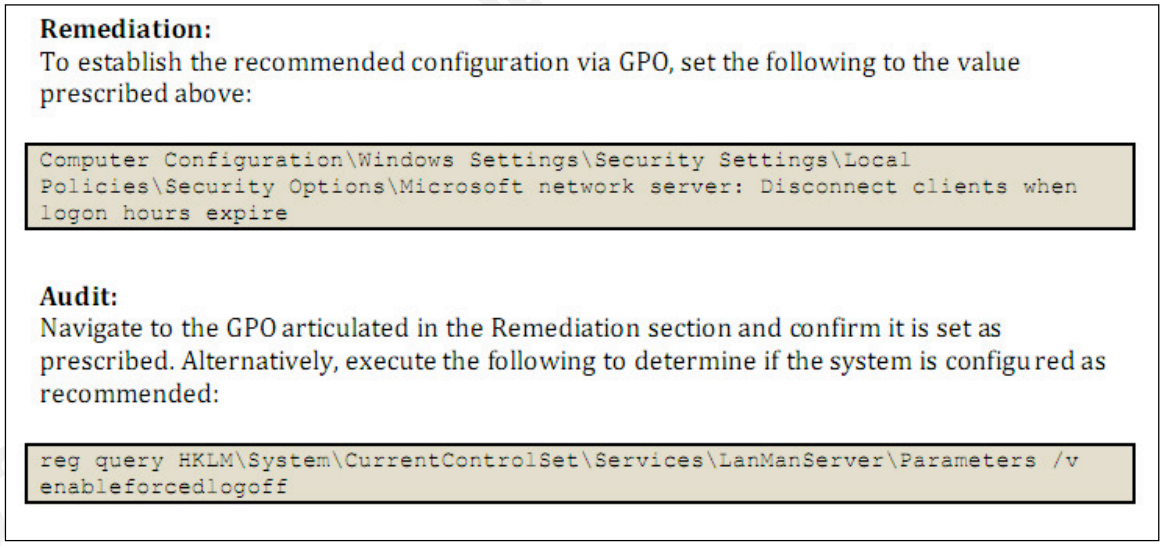
Driving the system is primarily via an intuitive web interface, there are fully featured web services available for those that which to integrate with other systems. Reporting is robust and delivered in various formats, including HTML, PDF, MHT and CSV.

2. Compliance Scanning with QualysGuard and CIS Benchmarks

2.1. Defining your policies

For the purposes of this example, the CIS Windows 2008 benchmark (Center for Internet Security, 2010) without modification will be used.

Ideally, there should be some discussion between the business and IT staff regarding an enterprises policies and standards. Where an organisation has policies and standards in place, you would then use those policies to establish your policy compliance tests within Qualys. When there are none, the CIS Benchmarks are a great starting point.


Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Disconnect clients when
logon hours expire
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
enableforcedlogoff
```

Figure 1 - CIS Benchmark Remediation and Audit advice

The CIS benchmarks include audit advice for each recommendation and Qualys have created tests for just about every single one. There are some caveats worth mentioning. Not all recommendations can be referenced via the windows registry, for instance many of the password

policy settings have no registry setting (Microsoft, 2009). These settings must be accessed either using direct host interactions (GUI or command line) or programmatically (Tenable Security, 2010).

Fortunately, Qualys have done the majority of the heavy lifting and have out of the box support wherever a recommendation can be remotely verified. There will be some settings either that cannot be remotely verified or that Qualys have not yet implemented. Considering the thoroughness of their work, I have often found the first condition to be the cause.

Where a custom test needs to be performed, you can create your own controls. We will verify that Symantec Anti-Virus is installed on the system by testing the appropriate windows registry key and the existence of the executable itself.

From this point on the focus will be on the practical side of performing policy compliance scanning, focusing on implementing the recommendations in the CIS Windows 2008 benchmark, Version 1.0 (Center for Internet Security, 2010).

2.2. Creating a QualysGuard Compliance Policy

Accessing QualysGuard is straightforward, simply point a web browser at https://qualysguard.qualys.com/ and follow the login prompts.

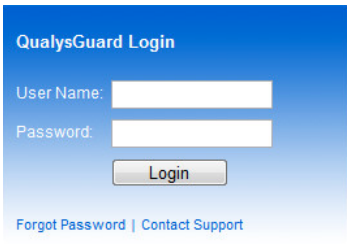


Figure 1 - The QualysGuard Login

The default-landing page after login is configurable. The default is a list of Vulnerabilities sorted by date last modified. There is an always-present menu on the left side. There is a selection of tools available such as Scan and Report, which will be used later. Before compliance scanning can be done, a policy needs to be created.

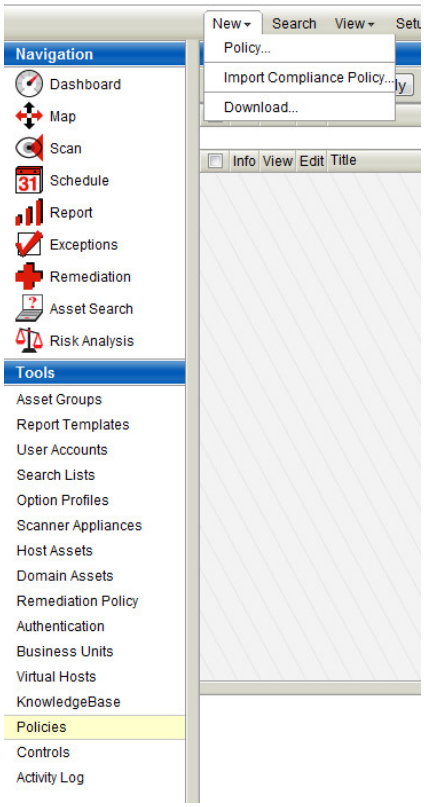


Figure 2 - Creating a new policy

On the lower left hand of the login screen is a link "Policies". Following that link will take you to an empty list of current policies, assuming you have never created any in the past.

2.2.1. Creating a New Policy

From this location, the "New" pull down menu will offer options specific to the current context, as you would expect from any application. "Import Compliance Policy…" will allow you to pull into your account policies that have been created by Qualys. "Download…" in this context will allow you to download the list of policies.

The "Policy…" menu item will open up the policy editor in a new window.

When creating a new policy, the system disables the policy editor screen and will prompt you to nominate the technologies that will be tested. By default the interface for searching and adding existing controls will limit the results to the technologies checked here. Windows 2008 Server has been selected, as this is the current focus. Clicking the OK button will set the technologies and activate the rest of the window.

Figure 2 - Setting Technologies

Stewart James stewart@stootles.com

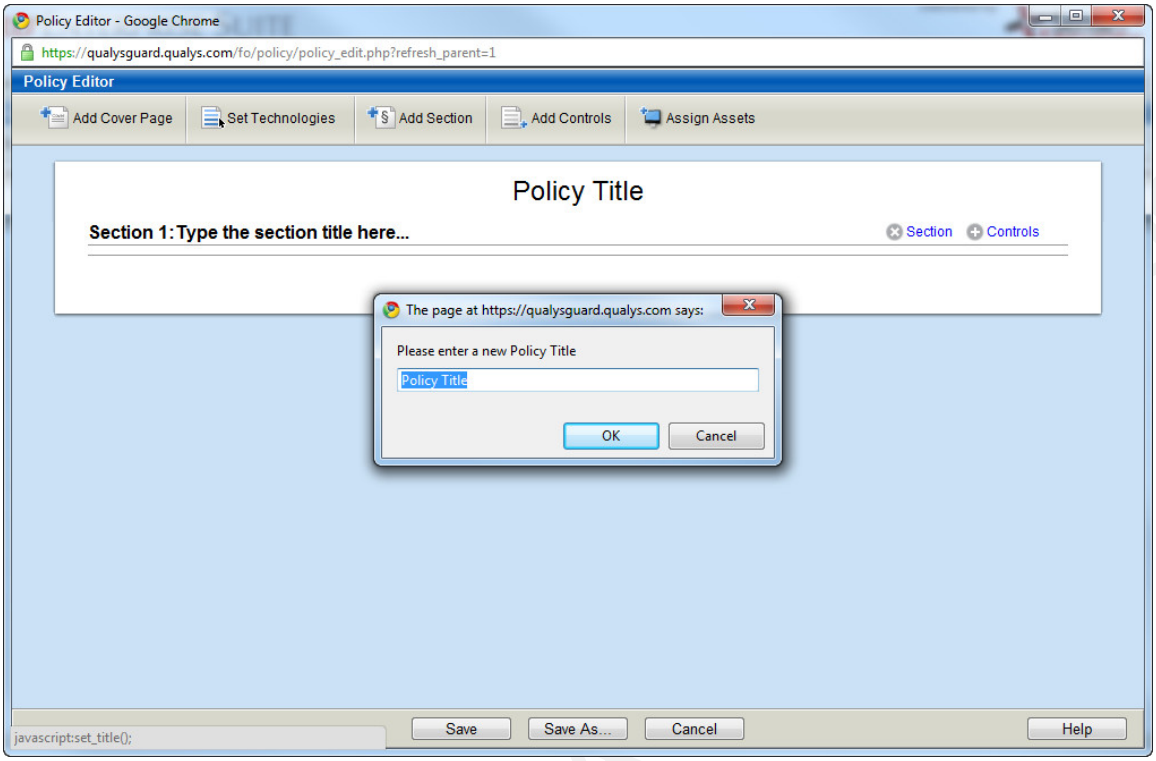


Figure 3 - The QualysGuard Policy Editor

The policy editor is straightforward to use and intuitive in the approach. There are five buttons along the top and are straightforward:

- Add cover page – allows you to create a free flow text cover page for the report
- Set Technologies – allows you to add or remove the technologies being targeted
- Add Section – allows you to add new sections to the policy
- Add Controls – allows adding tests to the policy
- Assign Hosts – allows you to define which hosts can use this policy

Clicking on the generic names, such as "Policy Title" and "Section 1: Type the section title here…" will open a JavaScript prompt and allow you to set the specific title.

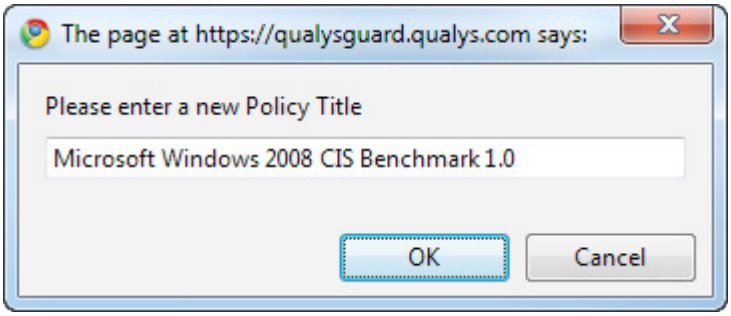


Figure 3 - JavaScript Prompt

Stewart James stewart@stootles.com

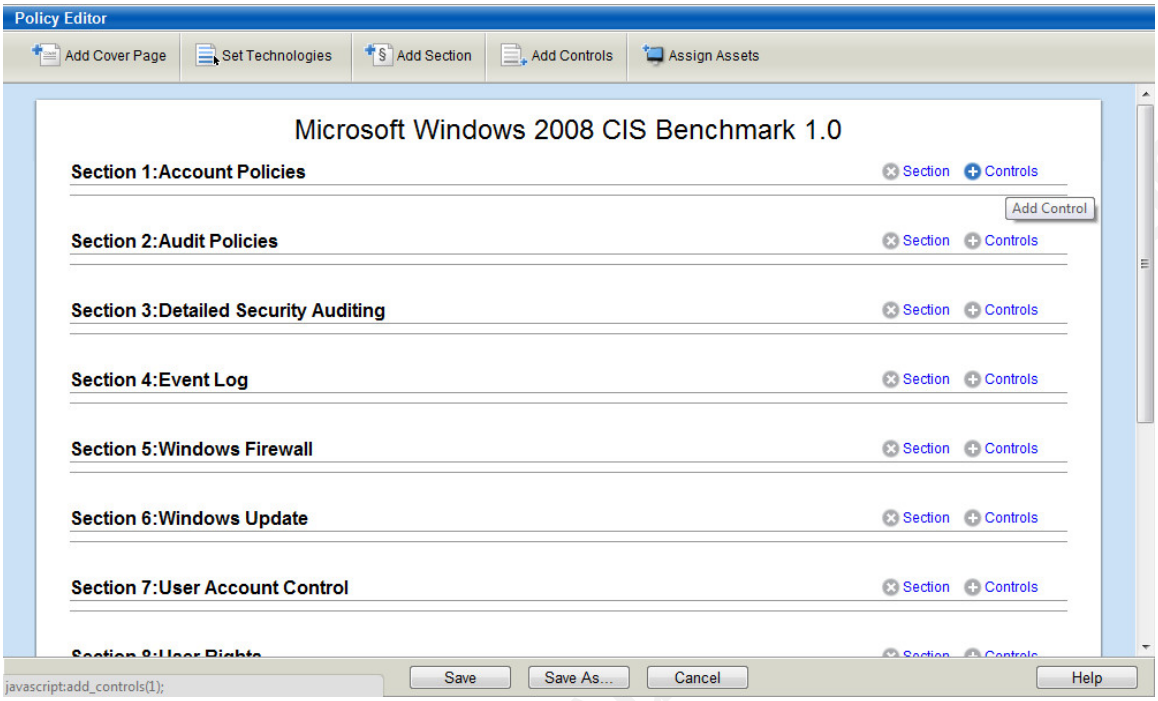


Figure 4 - Section titles mirroring CIS benchmark

The policies have some limitations, such as only one layer of sections. It is trivial to put these sections on par with the CIS benchmarks by ensuring the naming and numbering is similar. The key difference for the section numbers is that the CIS references have a leader 1.x for each section; this cannot be represented in the QualysGuard policy definition.

If a section needs to be relocated, click on the section number and enter the section number that should be assigned. Other sections will be moved up or down as appropriate.

2.2.2. Adding controls

The most direct method to add a control is to click on the "+ Controls" link to the right of the section header the control should be placed. This will open a window that allows you to select from the comprehensive list of existing controls. At the time of writing, over 500 were presented when the Windows 2008 technology was set.

Figure 4 - The "+ Control" link

Stewart James stewart@stootles.com

It is possible to check each control that is of interest and click the add button. This speeds up the process of importing each test, at the expense of time spent organising all the tests later. As the basis for these tests is the CIS recommendations, it is logical to ensure that each of the controls is in the same sequence as documented by the CIS. Making the reports readable and readily referable is important. To find a specific control, there is a search button at the top of the "Select Controls" window.

2.2.3. Searching controls

There are a comprehensive number of options for finding existing controls. The only options selected are those that match your technologies selected earlier. Which makes perfect sense as a policy targeting Windows probably does not need a Linux only test performed.

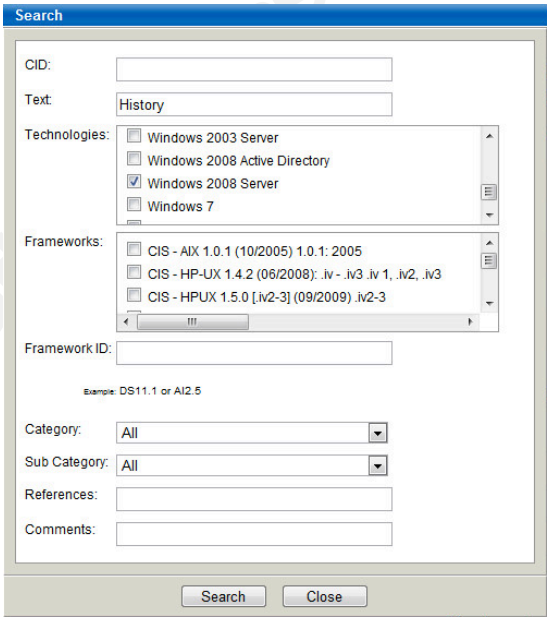


Figure 4 - Searching Controls

There are a few options available to finding specific controls. QualysGuard appears to let you do it the way you like. If you know the unique Qualys assigned Control ID (CID), you can enter that number and click search. Using the text field will allow you to search for any text that matches (such as history).

The defaults assigned to the Technologies field should be relevant to the current policy. The Frameworks field is interesting as you can limit your results to only a specific framework, such as a specific CIS benchmark or an International Standard. The native controls are very comprehensive and well referenced. When looking for a specific control, you can even refer to it by the associate framework reference number (Framework ID).

The "Maximum Password Age" recommendation in the CIS Windows 2008 benchmark has an ID of 1.1.2. If I put 1.1.2 into the Framework ID section, ensure that Windows 2008 is

selected in Technologies field and that "CIS – Windows 2008, 1.0 [Member Server]" is selected in the Frameworks field a very small number of results will be returned.

You can further restrict search results down to a specific category or sub-category of control. You are also able to search on the reference and the comment fields. The content in these fields is user driven and are not managed by Qualys. Within any account, an appropriately authorised user can add references and comments to any existing control.

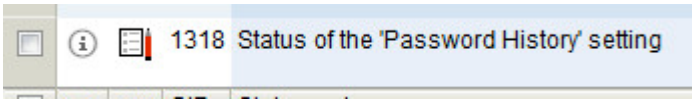


Figure 4 - Selecting a control

Once you have found the control you are looking for select the checkbox to its left and click add.

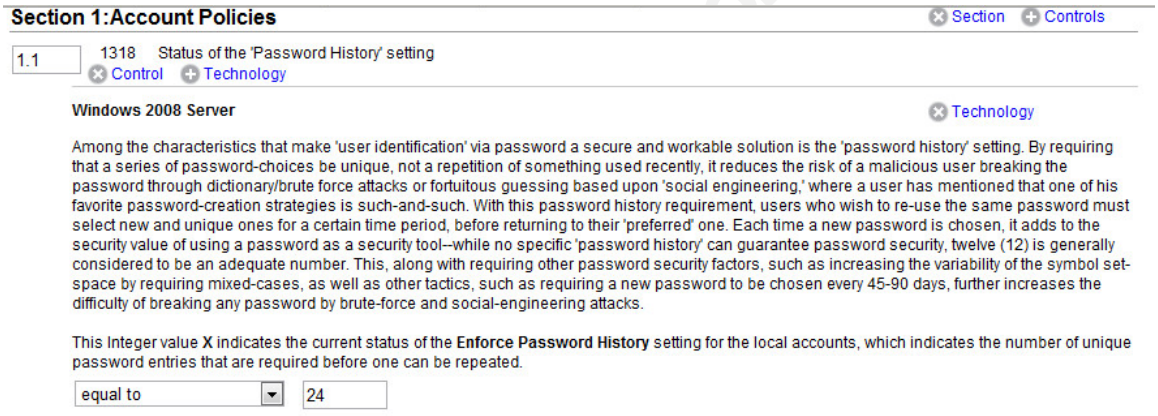


Figure 5 - The control now added to the policy

Stewart James stewart@stootles.com

2.2.4. Fine Tuning and Reorganising Controls

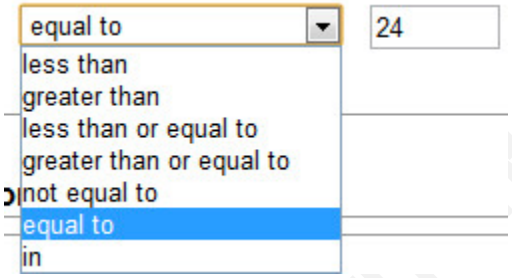


Figure 5 - Customise a control

The built in control defaults may need to be adjusted to suit a particular environment. Qualys allows for customisation of each control, depending on the expected date type.

Just like sections controls can be moved around simply by changing their number and either pressing TAB or clicking somewhere else on the page. You can also move a control to a different section (change control 1.4 to 4.1) and within a section (change control 1.4 to 1.2). Control numbering must be sequential and no number can be skipped. QualysGuard will alert you if the number you select is inappropriate.

2.2.5. Wash, Rinse Repeat – Save Often

The most time consuming part of policy creation is creating the initial policy. It can take a while to find and add all the controls and to ensure that the controls are in a sequence you believe to be suitable.

Do not forget, until you click the "Save" button, none of your work is saved. If you are building a comprehensive policy, do not forget to save frequently to ensure you do not lose any of your work.

2.3. Creating Custom Controls

As helpful as Qualys is at giving you built in controls for many of the CIS tests, some are not yet covered and sites may have some specific requirements. You can create custom controls to satisfy a significant number of tests. Potential control types for the windows platform are:

- Registry Key Existence
- Registry Value Existence
- Registry Value Content Check

Stewart James stewart@stootles.com

- Registry Permission
- File/Directory Existence
- File/Directory Permission
- File Integrity Check

This wide range of tests should be able to perform the majority of work needed on the windows platform. The only item lacking is the ability to check for specific file contents, which is available in the UNIX control types.

2.3.1. Testing for the presence of Symantec Endpoint Security

There are a number of obvious ways to test for installed software, the presence of a file, the hash value of that file, the presence of a specific registry key or a registry value. Setting aside all the arguments available for or against different methods, I will be simply looking for the presence of a specific registry key and the existence of a file.

It is worth taking note that in the vulnerability-scanning portion of QualysGuard you can request QualysGuard report on whether or not specific services are running or even specific network ports. This is not possible with compliance reports and is of course an even better approach to ensuring something such as Anti-Virus Software is running.

The process is very simple. All controls are viewable by selecting “Controls” in the left hand Tools menu. This interface allows you to search and review the available controls. Clicking the “New” pull down menu and selecting “Control…” opens a wizard like interface.

Stewart James stewart@stootles.com

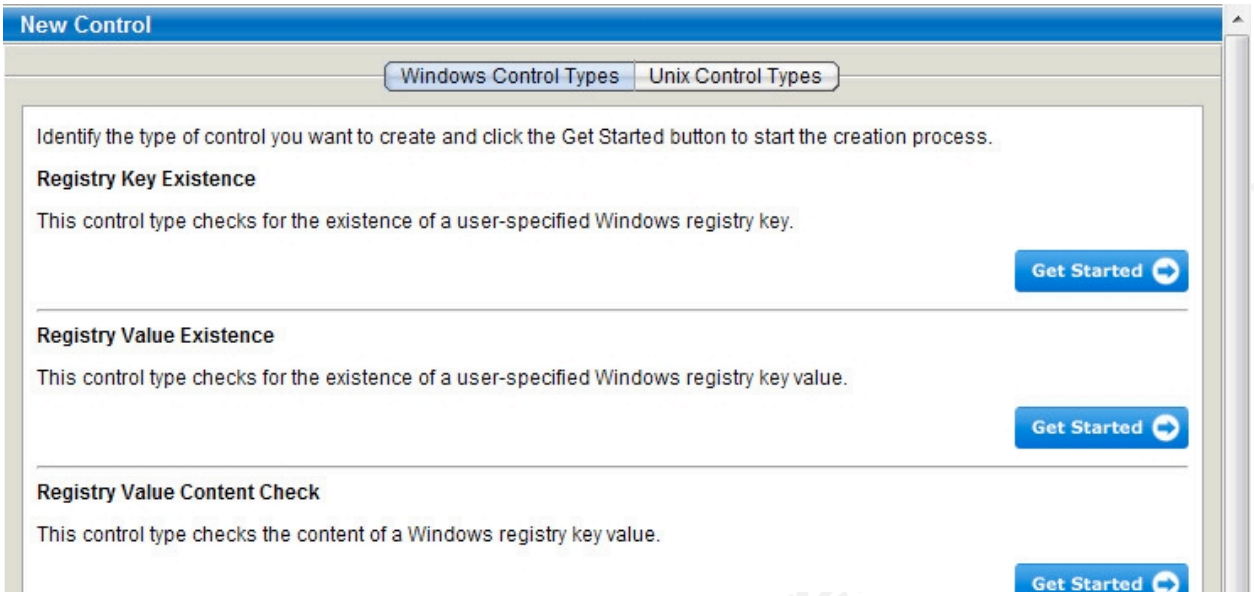


Figure 5 Creating a custom control

Simply selecting the "Control Type" and then an appropriate "Get Started" button will take you to the next and only additional screen. You are then presented with a single form asking for details such as what will actually be tested such as what category the test is, why that test is taking place and the rational. If there are any relevant references, they too can be included for presentation when reporting. Qualys will issue your control with a Control Identifier (CID). With custom controls, the CIDs are issued numbers starting at 100000 to help ensure you can easily identify Qualys controls as opposed to your organisations custom controls.

The custom tests are very straightforward. As stated, a test for a specific registry key and then a specific file will be used to verify that Symantec Endpoint is installed.

- Registry Key Existence
  - Test for HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Security
  - Response is True
- File/Directory existence
  - Test for C:\Program Files\Symantec\Symantec Endpoint Protection\smc.exe
  - Response is True

There are complete screen shots available in the appendix for those wanting to see the full details of either custom control.

Stewart James stewart@stootles.com

Adding these controls is the exact same process as adding the included controls to your policies. In this instance a new section labelled “Local tests” has been create and these 2 controls added to that section.

2.4. Creating a Compliance Scanning Profile and Authentication Records

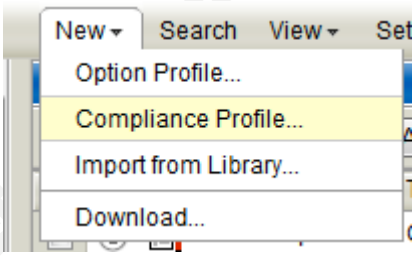


Figure 5 Creating a new profile

Qualys uses profiles to identify different scan types. There are two broad types. One profile type is for vulnerability scanning and network mapping. The other profile type is for performing compliance scans. This allows you to perform different types of scans depending on the current requirements. While there are many options for vulnerability and mapping, the requirements for compliance scanning is quite straightforward.

Starting a new compliance file follows a logical series of actions, as is typical of QualysGuard. Under the Tools menu, select Option Profiles and then click on the New pull down menu and select compliance profile.

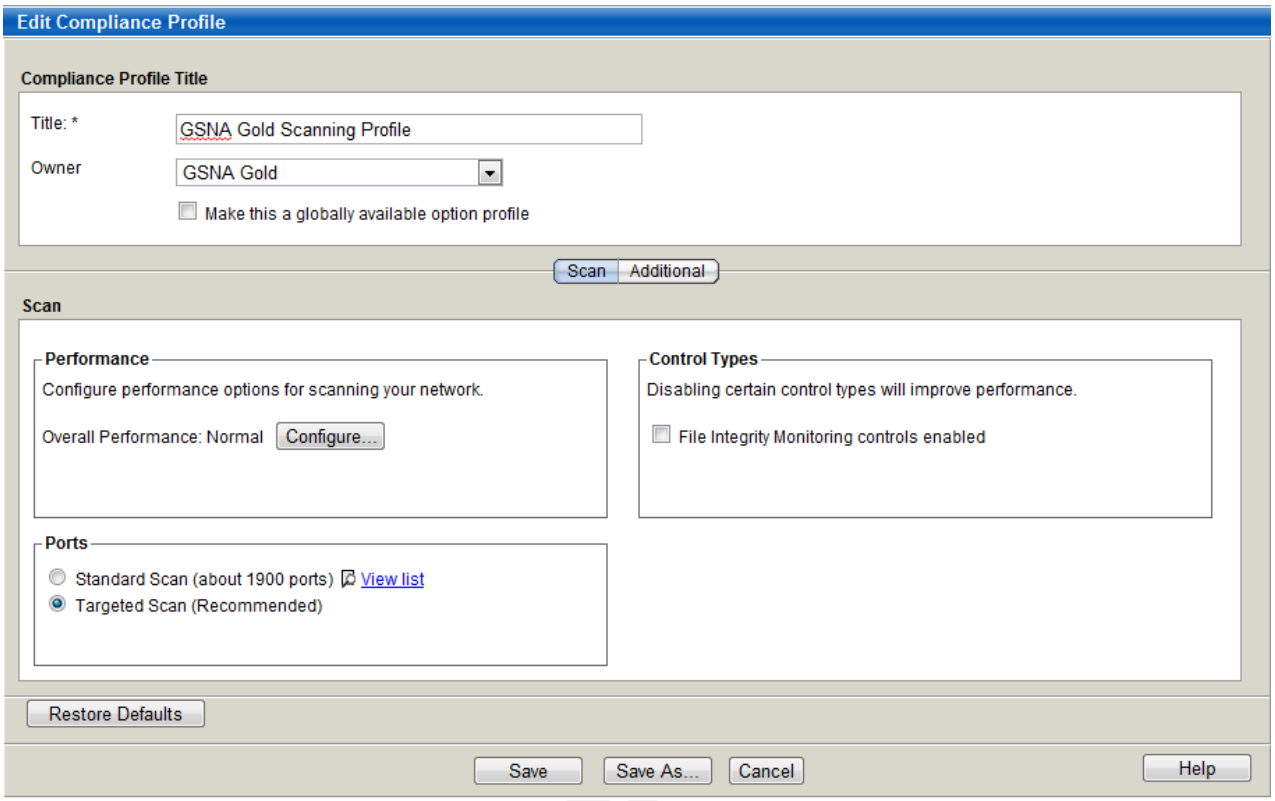


Figure 6 Creating or editing a Compliance Profile

For this example, the default settings are suitable. The profile defines how QualysGuard will identify hosts of interest, detect they exist and what their OS is. There are additional settings for informing how it should handle certain network events that a firewall between QualysGuard and the target host will cause and, importantly, any ports you want to make sure QualysGuard does not probe. Give the profile a name and commit it by pressing save.

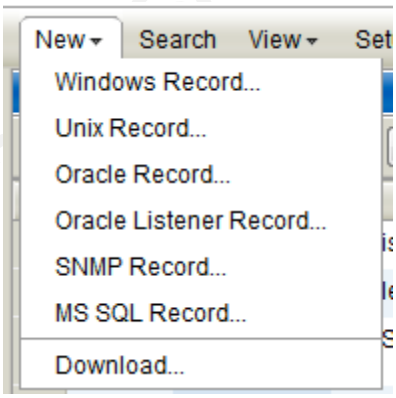


Figure 6 Many authentication types

One other piece is required before a scan can be performed.

Compliance scanning requires local access to a given machine. Qualys must be able to authenticate to a system with suitable privileges to perform many of the tests. As we are interested in windows hosts, we will focus on creating a windows record for a standalone system. Again, Qualys has placed this section under Tools with the logical feature title of

Authentication Records. Figure 17 shows the array of authentication types QualysGuard understands.

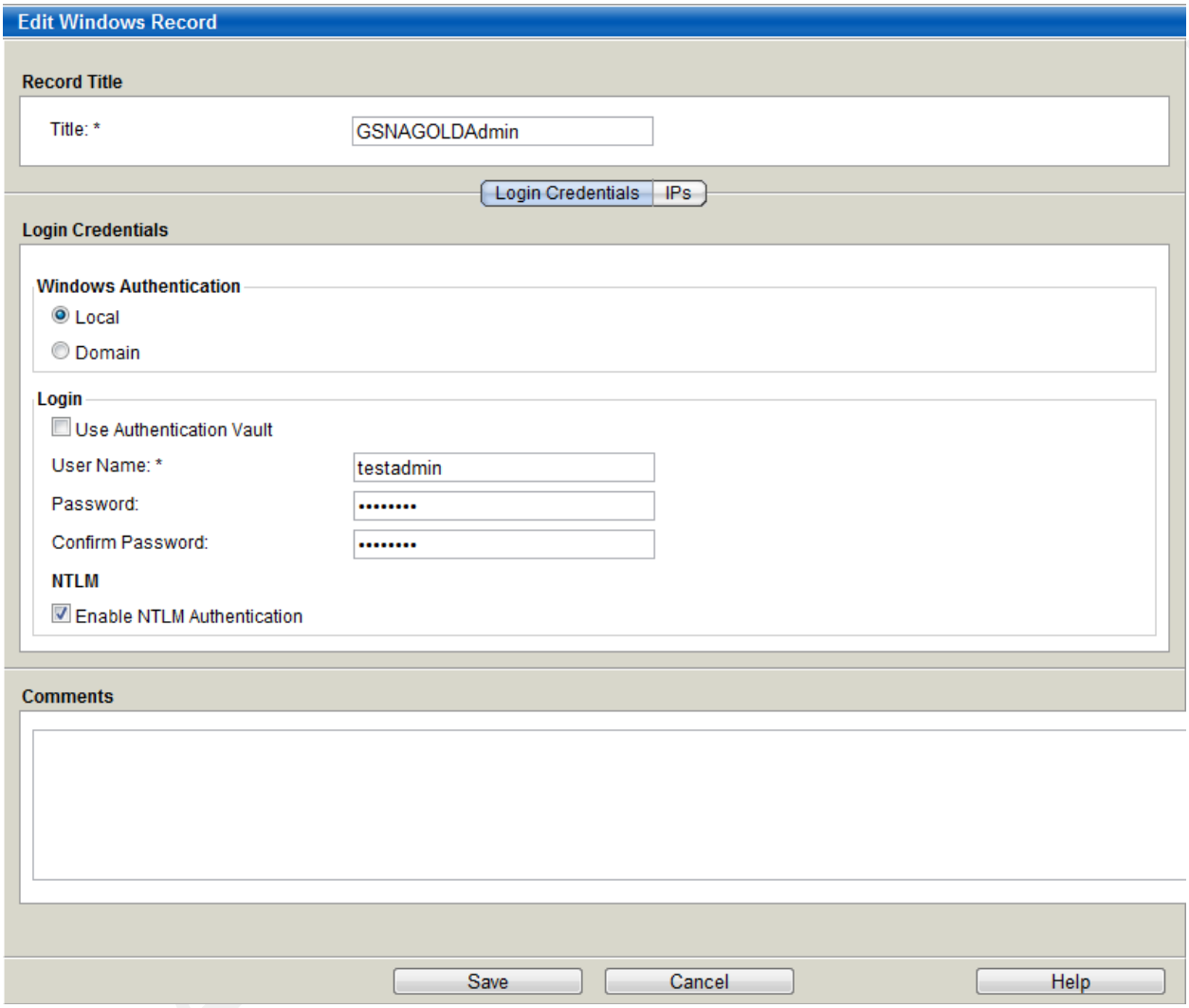


Figure 7 Creating/Editing an Authentication Record

Authentication records for standalone systems are straightforward. Qualys simply requires a username and password, for windows hosts you also have the option to allow (or not) NTLM authentication. This is on by default, if you want to ensure only potentially more secure protocols such as Kerberos are permitted simply uncheck the appropriate option.

Stewart James stewart@stootles.com

Finally, Qualys needs to be told which hosts to use this record on. This makes sense as if Qualys had to try 20, 50 or 100 different username and password pairs it may lock accounts before it is successful. This can be done manually (entering the systems IP address) or if you are grouping systems in the QualysGuard as discussed in Tim Proffits paper "Creating a comprehensive Vulnerability Assessment Program for a Large Company Using QualysGuard" (Proffit, 2008), and those hosts will all have an identical suitable account available, you can link an authenticated record with a specific group.

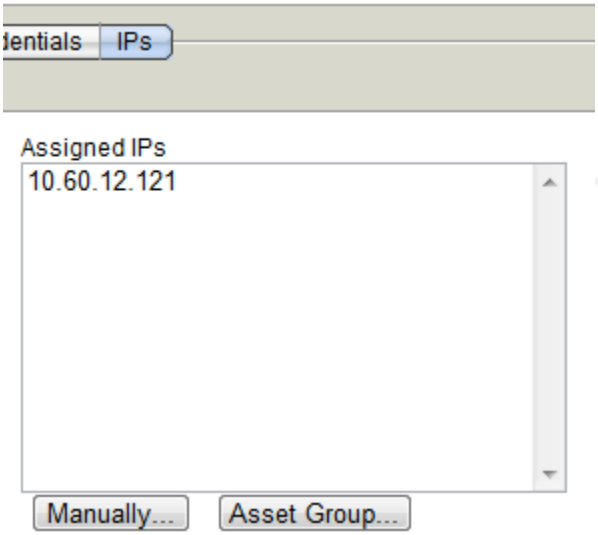


Figure 7 Assigning systems to Authentication Records

With an option profile, authentication records in place and the policy definition created earlier, the system is ready to go. It is now possible take full advantage of the QualysGuard system and begin scanning and reporting.

2.5. Running a compliance scan

All the heavy lifting is now out of the way. With the above steps completed, you can now perform a compliance scan simply by launching a new compliance scan.

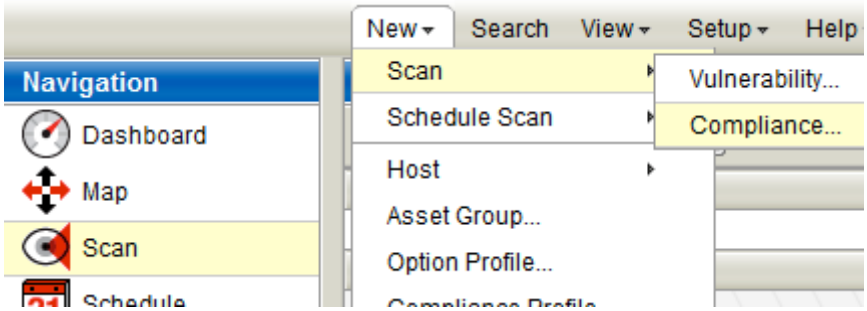


Figure 7 Performing a compliance scan

The compliance scan window at this point is very simple. It will ask for a small number details:

- A title for your scan
- Which compliance profile to use
- Which scanner appliance to use (you may have many actual scanner appliances)

Stewart James stewart@stootles.com

- You can then specify an Asset Group or specific IP addresses you want to scan.

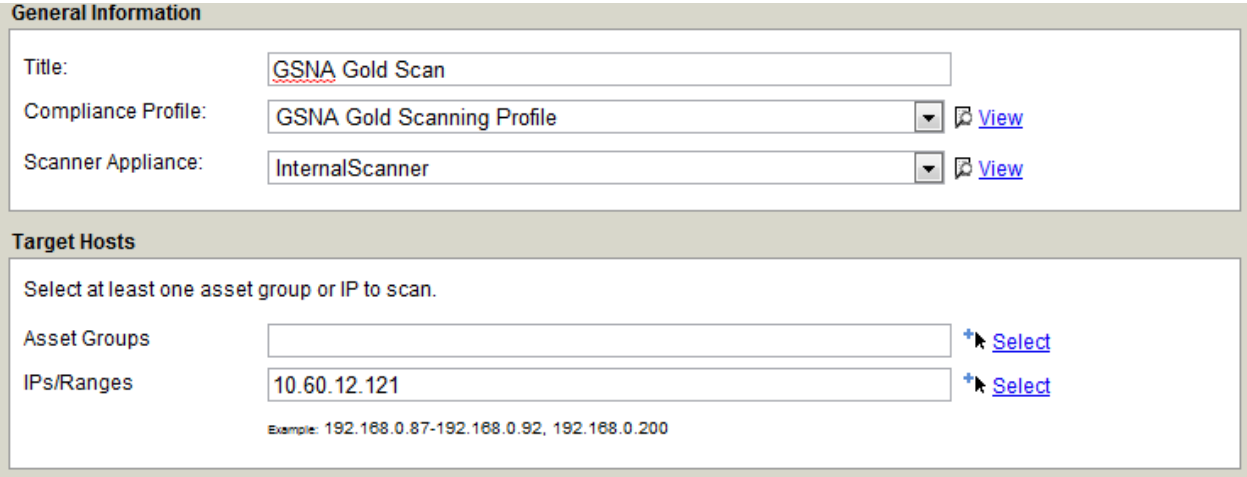


Figure 8 The last screen before a scan is finally launched

2.5.1. Scheduling regular scans

Scheduling regular scans is a trivial task. As well as requiring the information for a once off scan, options concerned with the scheduling and notification are available. The scheduling offers similar capabilities to recurring appointments in a calendar application.

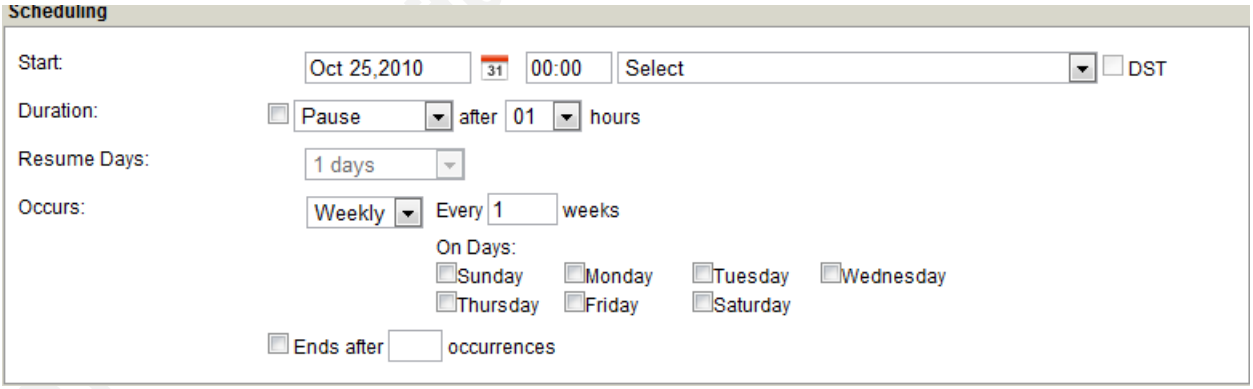


Figure 9 Just like a corporate calendar, regular scans are straight forward

Qualys allows you to set a time limit for a scheduled scan and then configure actions to be performed when that time limit is reached. For example, if a scan takes more than 1 hour to complete you could cancel the scan. Alternatively, you could configure Qualys to wait for 1 to 9 days and then continue the scan.

Stewart James stewart@stootles.com

The Notification settings are basic and allow you to send a reminder to the task owner from 5 minutes and up to 31 days before the scheduled scan starts. You can send these notices to additional email addresses and add a custom comment to the emails. These notices are most useful to ensure that all relevant people are notified of an impending scan.

In the SANS Auditing Networks, Perimeters, and Systems Course (SANS, 2010b) it is recommended that when performing an audit, all relevant people should be notified. This feature can and should be used to ensure that prior notification is presented and the comment field could be used to ensure that staff have suitable contact details in case of an emergency caused by the scanning.

2.6. Reporting on results

Once a scan is complete, you need to use the Report section of QualysGuard to generate meaningful results. Unlike vulnerability scans, Compliance scans results are a just a summary of the scan that was performed, no details about the individual tests are supplied.

The compliance reporting system has two main types of reports, template and interactive.

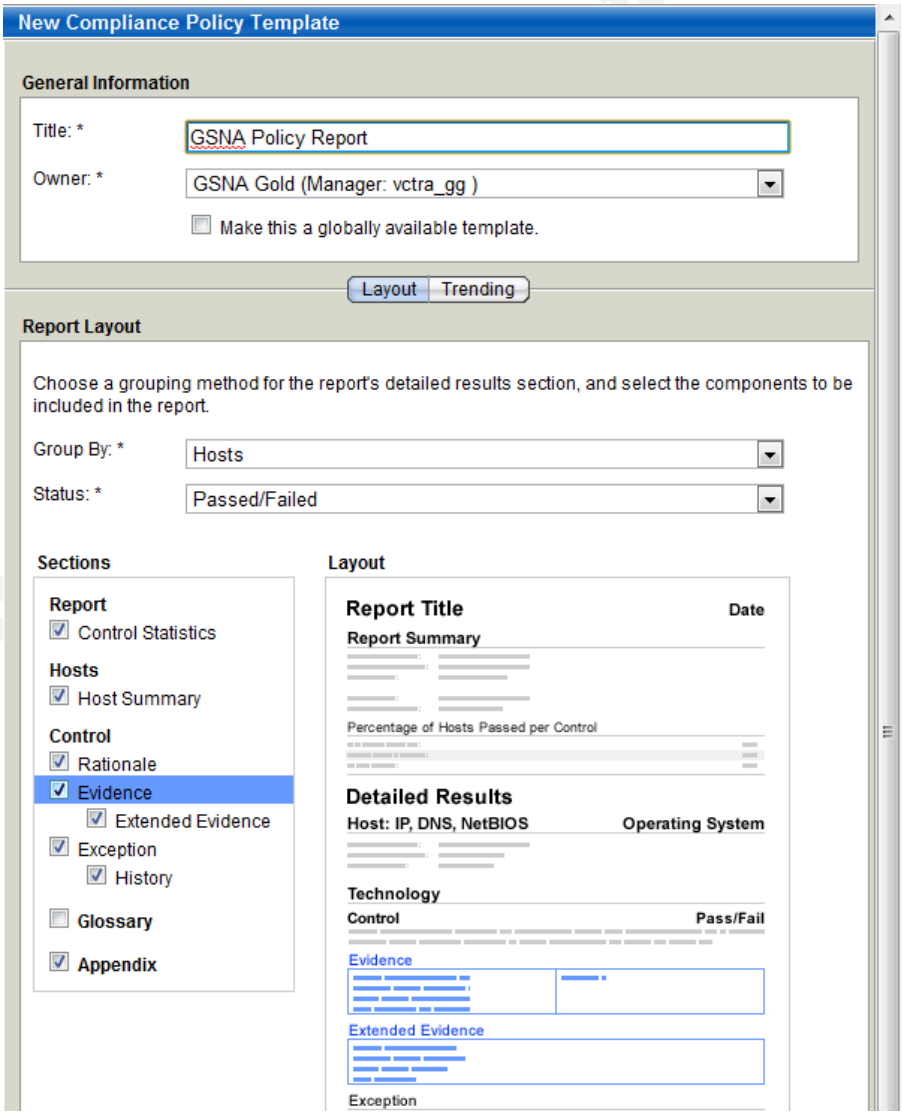
- Template Reports – Reports are static and stored in a format such as PDF or HTML
    - Authentication Report – The Authentication Report identifies whether authentication to hosts was successful for the most recent compliance scans. This is an important tool as successful authentication is a requirement for compliance scanning. (Qualys, 2010c)
    - Policy Report – The Policy Report identifies compliance status for a specific policy. A user created template is required for this report type. (Qualys, 2010c)
- Interactive Reports – are interactive and used to request audit exceptions
    - Control Pass/Fail Report – The Control Pass/Fail Report identifies the compliance status for a particular control. When you run this report, you will specify a policy and a control from that policy to report on. Hosts are listed with a pass or fail status for the specified control. (Qualys, 2010c)
    - Individual Host Compliance Report – The Individual Host Compliance Report identifies the compliance status for a particular host. When you run this report,

you will specify a policy and a single host to report on. Each control from the policy that is applicable to the host is listed with a pass or fail status for the host. (Qualys, 2010c)

Stewart James stewart@stootles.com

2.6.1. Creating a policy report template

As stated above, template reporting requires a user created Template. Select “Report Templates” from the left hand menu, click “New” then “Policy Template…” from the pull down menu. You are given a simple screen asking for a title, how you would like the results in this report grouped (hosts or controls), whether to display passed, failed or both control statuses and then which sections should be included. As can be seen in the screen capture below, if you hover over a section it will highlight in blue in the “sample” report on the right. For our purposes, we will be accepting the defaults and clicking save.



Stewart James stewart@stootles.com

Figure 10 Creating a Policy Report Template

2.6.2. Running a template report

Template based reports are useful for creating a static report to be sent to a third party. There are a few out of the box reports available. SANS Top 20 Report, Qualys Top 20 Report, *Policy Report*, Payment Card Industry (PCI) Executive Report, and Payment Card Industry (PCI) Technical Report.

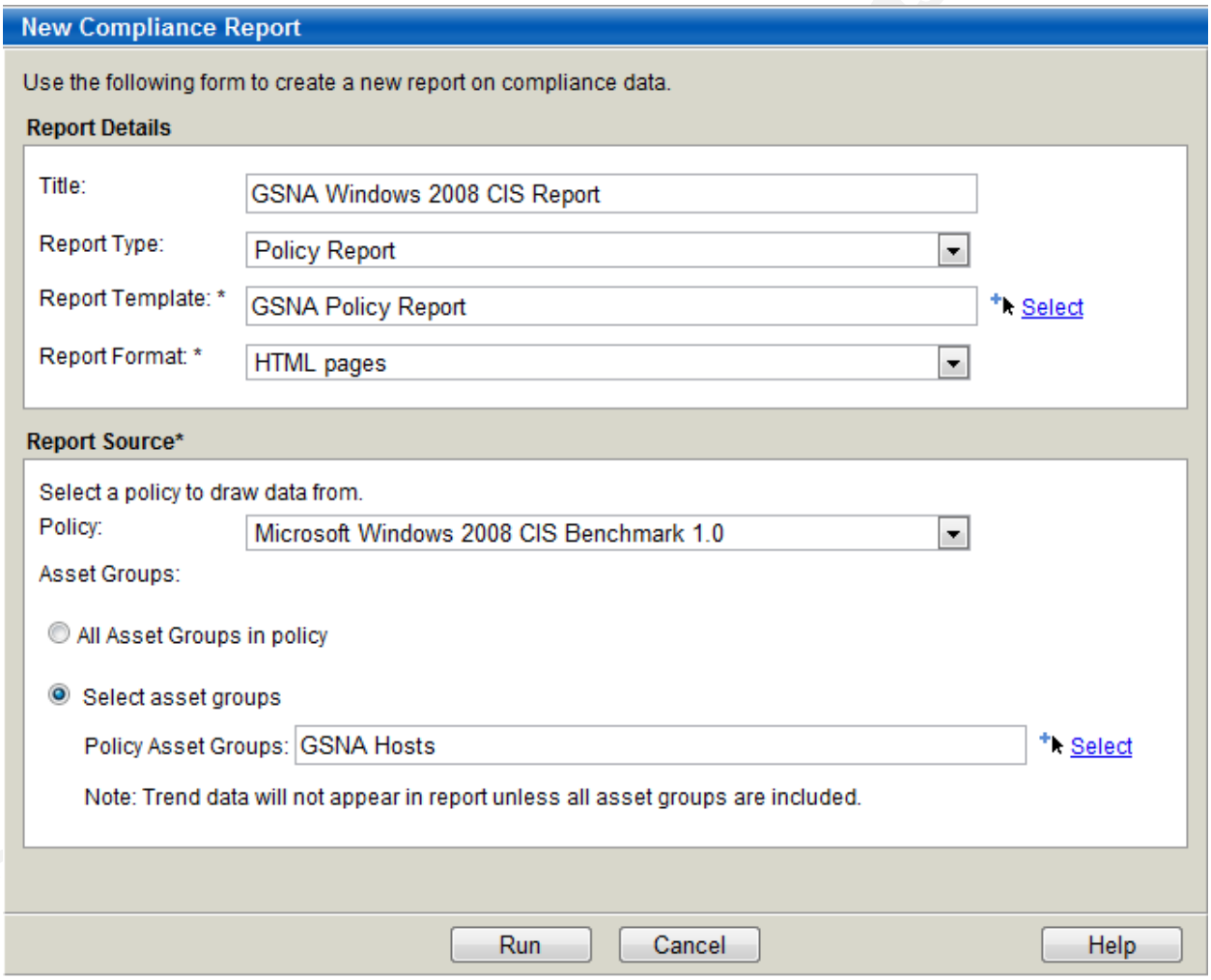


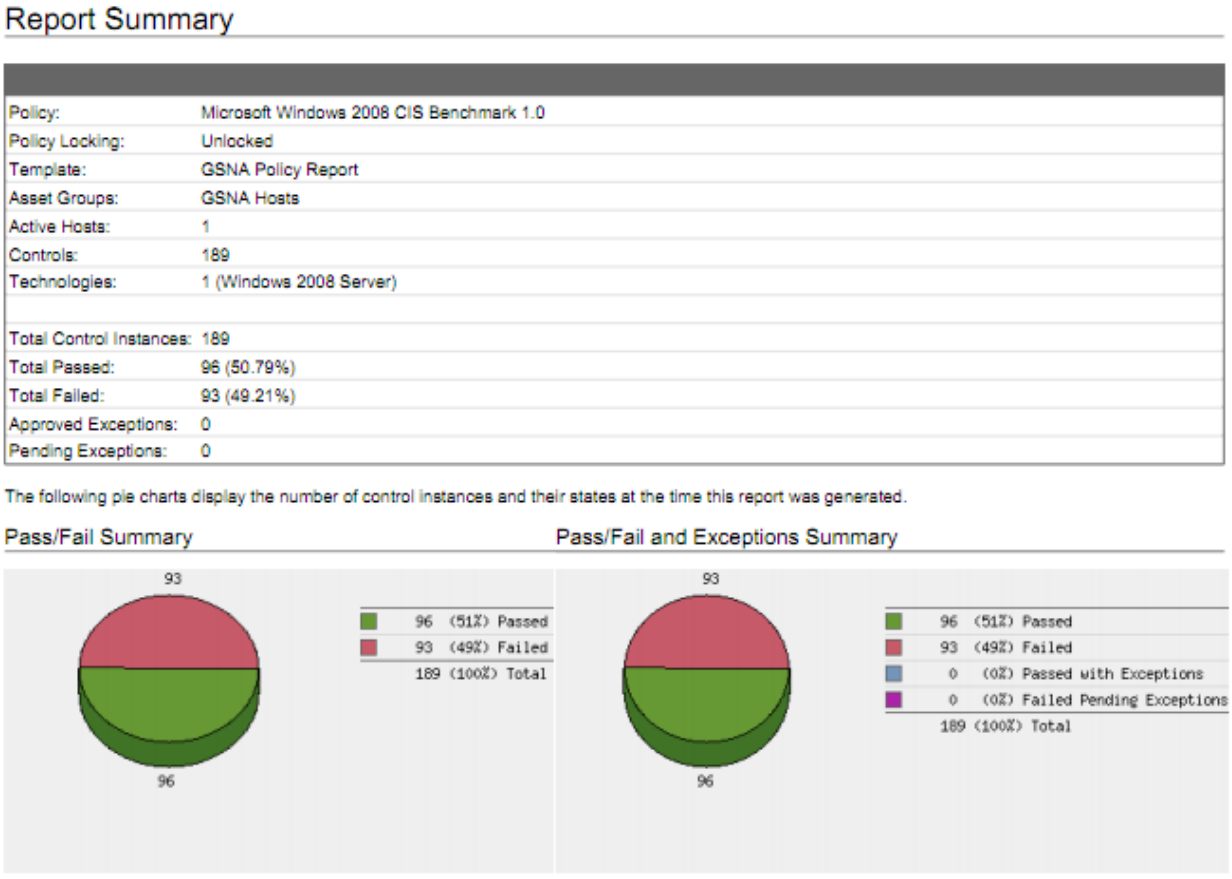
Figure 11 Running a Template Report

Policy Report allows you to select a Report Template. This report template combined with the selected policy and then filtered to include relevant assets will then generate your report.

Stewart James stewart@stootles.com

Entering appropriate options and clicking run will cause Qualys to begin generating the report. Depending on your Report Format (HTML, PDF, MHT, CSV, XML), your browser will either display or prompt you to save the report. The default report is extremely detailed. The report for this one host in PDF format is 62 pages.

At the top of the report is a *summary*. This summary states the high-level pass/fail statistics and offers a couple of pie charts as a visual aide. The system does differentiate between a failed control and a failed control that has an exception, which is why there are two different pie charts. As we have not yet requested any exceptions or approved any, these figures remain at zero.



Report Summary

Policy:	Microsoft Windows 2008 CIS Benchmark 1.0
Policy Locking:	Unlocked
Template:	GSNA Policy Report
Asset Groups:	GSNA Hosts
Active Hosts:	1
Controls:	189
Technologies:	1 (Windows 2008 Server)
Total Control Instances:	189
Total Passed:	96 (50.79%)
Total Failed:	93 (49.21%)
Approved Exceptions:	0
Pending Exceptions:	0

The following pie charts display the number of control instances and their states at the time this report was generated.

Figure 12 The template report summary

The next section is *Control Statistics*. These are the controls listed in the order defined in the Compliance Policy. This section is succinct, stating the control ID, a short statement, a pass

rate in percentage as well as the actual figures for number of hosts that passed out of how many were tested.

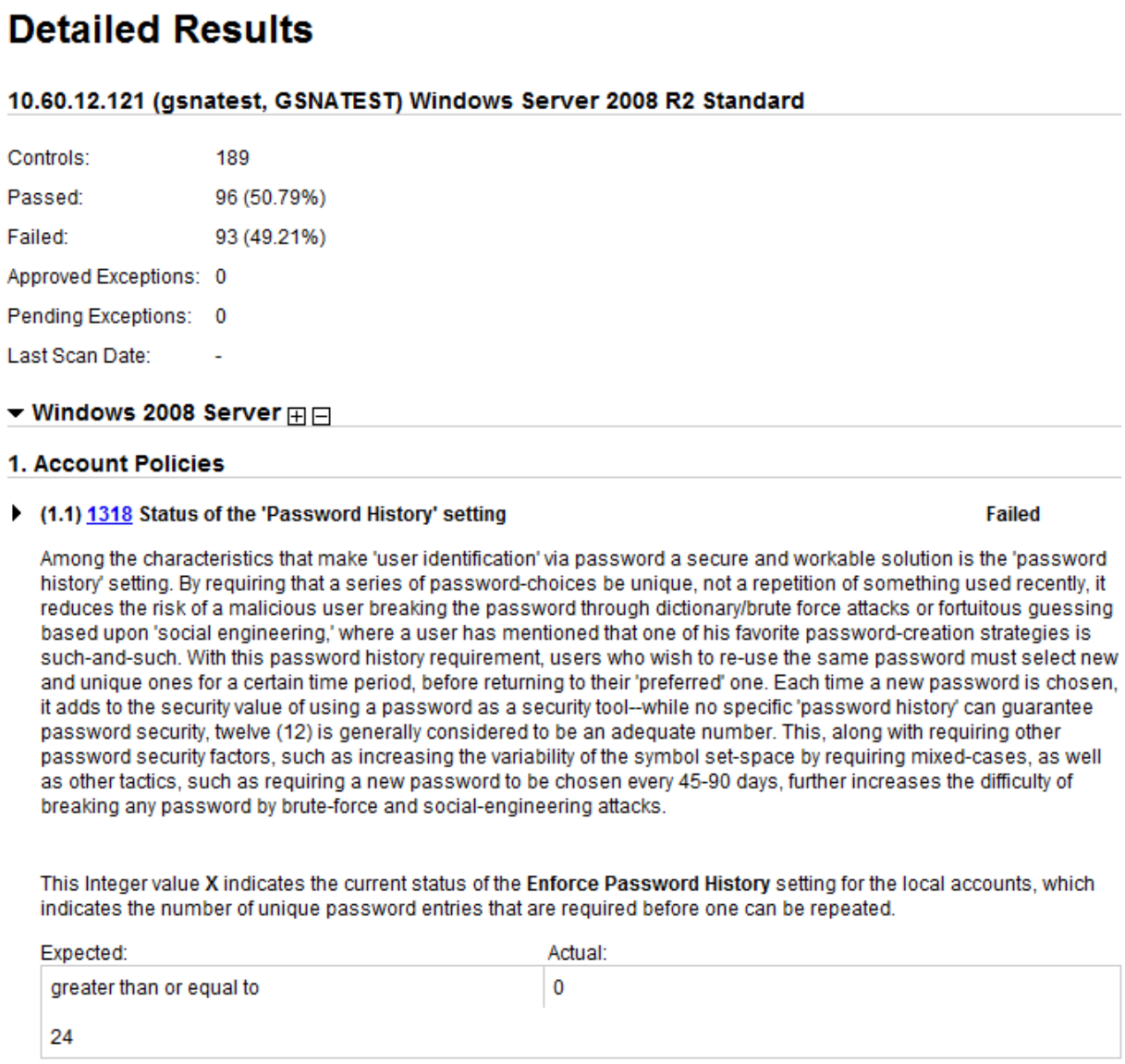
1. Account Policies

Order	Control ID	Statement	%
1.1	1318	Status of the 'Password History' setting	0% (0 of 1)
1.2	3376	Status of the 'Maximum Password Age' setting (expiration)	100% (1 of 1)
1.3	1072	Status of the 'Minimum Password Age' setting	0% (0 of 1)
1.4	1071	Status of the 'Minimum Password Length' setting	0% (0 of 1)
1.5	1092	Status of the 'Password Complexity Requirements' setting (Guidance= Enable)	100% (1 of 1)
1.6	2484	Status of 'Store passwords using reversible encryption' setting	100% (1 of 1)
1.7	2341	Status of the 'Account Lockout Duration' setting for invalid login attempts	100% (1 of 1)
1.8	2342	Status of the 'Account Lockout Threshold' setting for invalid logon attempts	0% (0 of 1)
1.9	2343	Status of the 'Reset Account Lockout Counter After' setting	0% (0 of 1)
1.10	1382	Status of the 'Microsoft Network Server: Disconnect clients when logon hours expire' setting	100% (1 of 1)
Order	Control ID	Statement	%

Figure 13 Pass/fail status for individual controls

Following on are the detailed results. These results list the status of each host, starting with a summary for a given host and then the specific details of each control, the status (pass/fail), the detailed rational for the control, the expected result from the test and the actual result.

Stewart James stewart@stootles.com



Detailed Results

10.60.12.121 (gsnatest, GSNATEST) Windows Server 2008 R2 Standard

Controls:	189
Passed:	96 (50.79%)
Failed:	93 (49.21%)
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	-

Windows 2008 Server

1. Account Policies

(1.1) 1318 Status of the 'Password History' setting **Failed**

Among the characteristics that make 'user identification' via password a secure and workable solution is the 'password history' setting. By requiring that a series of password-choices be unique, not a repetition of something used recently, it reduces the risk of a malicious user breaking the password through dictionary/brute force attacks or fortuitous guessing based upon 'social engineering,' where a user has mentioned that one of his favorite password-creation strategies is such-and-such. With this password history requirement, users who wish to re-use the same password must select new and unique ones for a certain time period, before returning to their 'preferred' one. Each time a new password is chosen, it adds to the security value of using a password as a security tool--while no specific 'password history' can guarantee password security, twelve (12) is generally considered to be an adequate number. This, along with requiring other password security factors, such as increasing the variability of the symbol set-space by requiring mixed-cases, as well as other tactics, such as requiring a new password to be chosen every 45-90 days, further increases the difficulty of breaking any password by brute-force and social-engineering attacks.

This Integer value **X** indicates the current status of the **Enforce Password History** setting for the local accounts, which indicates the number of unique password entries that are required before one can be repeated.

Expected:	Actual:
greater than or equal to 24	0

Figure 14 Detailed results of a compliance report

As is seen from these short samples, the amount of information available is substantial. As the reporting and testing are performed in distinctly different steps, this will enable an auditor to generate different reports for different audiences. Allowing management to receive a high-level summary and for the specific administrators to receive detailed reports about their hosts.

The detailed reports offer specific reasoning and may be considered a third party and allow for a more cohesive relationship between auditor and an administrator. This enables a more robust and

open conversation between auditor and administrator as the administrator does not feel "they" are being reviewed. (SANS, 2010b)

2.6.3. Running and using interactive reports to record audit exceptions

Interactive reports allow you to review the pass/fail rate of a specific control or review a specific host against a specific policy. To generate an interactive report, follow a similar process as used for template reports (Reports->New->Compliance Report->Interactive). Choose either "Control Pass/Fail" or "Individual Host Compliance". Both will move forward requesting further information such as which host or which control, which policy, what do display and sorting preferences.

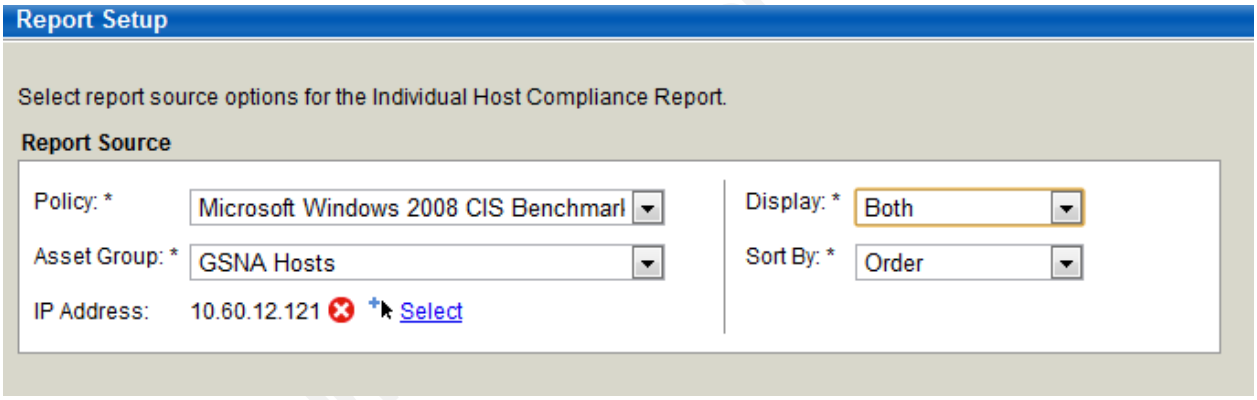


Figure 15 Preparing for an interactive report

Interactive reports offer similar information except for the high-level summary available in the template style report. The window is split into two main sections. The upper section is a brief overview of each control tested and its status. When you click on a listed control, the lower section is filled with the rational for the control, the expected result and the actual result.

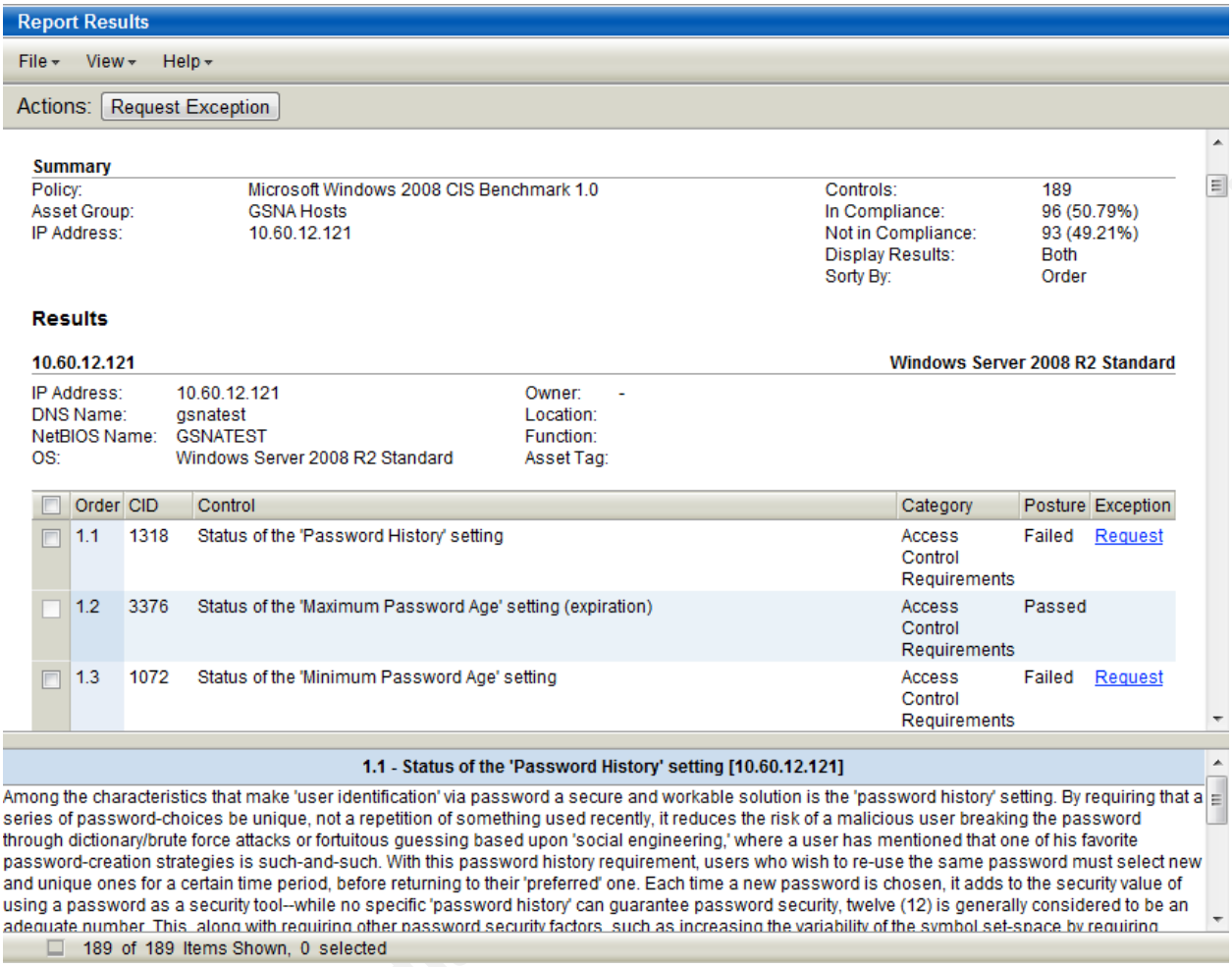


Figure 16 Interactive report

Observant readers will note that there is a column labelled “Exception”. When a control fails and it is acceptable or believed to be acceptable for that control to fail in that instance it is important to document that fact. Qualys allows for a simple workflow that permits a user to request an exception and then a manager to approve or reject that exception.

Stewart James stewart@stootles.com

2.6.4. Reporting on exceptions

QualysGuard provides a mechanism for reviewing and reporting on exceptions in its own menu option down the left hand side of the screen. This is very straightforward and shows which hosts have exceptions. An exception can be requested, approved, rejected or expired. While a host has an approved exception, the individual test is considered passed by QualysGuard.

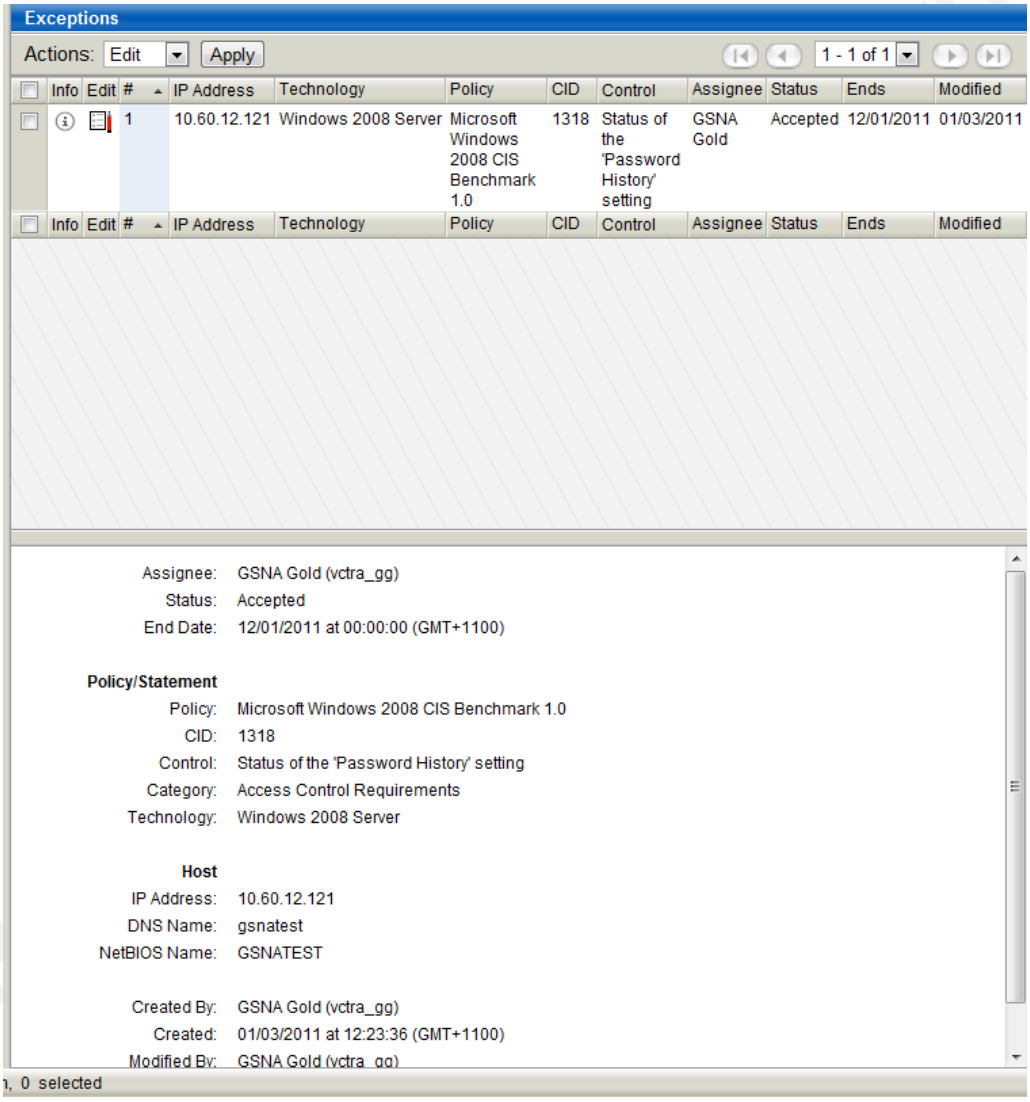


Figure 17 Reviewing exceptions

You are able to drill down into the exceptions and identify who requested the exception and their comments, as well as who approved the exception and their comments. Editing an

exception will allow for additional comments to be made as well as an optional change in the status of the exception.

3. Conclusion

Ensuring hosts remain configured as expected is an important part of information security. Ongoing regular measurement of such configurations can help administrators and management in identifying issues in a timely, consistent manner.

Toolsets, which require manual intervention to perform testing, are extremely useful in a small environment or where a small number of hosts are examined on an ad hoc basis. Such tools will not scale well when hundreds of hosts need to be examined. This scaling problem is greater when there is an expectation that such tests will be performed regularly.

This paper has highlighted the commercial offering from Qualys, QualysGuard. QualysGuard is comprehensive in its offering and continually improving. The SaaS model means there is no maintenance overhead for the security professional and a focus on making use of the tool is immediate and constant.

QualysGuard does have an increased overhead in initial configuration for compliance scanning when compared to some other tools, such as the CIS tool. Once this initial configuration overhead is performed, QualysGuard can be used to frequently scan and rescan as many hosts as required. Allowing the security professional to focus on the data being collected by QualysGuard rather than manually performing the scan.

The CIS benchmarks are comprehensive in their explanations and provide an excellent starting point for any organisation standardising their security configuration. When combined with an automated tool such as QualysGuard, it can aide an organisation in ensuring a large number of systems configured as expected and with regular automated scanning remain configured.

Policy compliance scanning can be a tedious, repetitive task. Any tool that automates this scan will aide an organisation in ensuring it is and remains configured as it expects.

Stewart James stewart@stootles.com

4. About the Author

Stewart James has worked at a major educational institute for over 10 years, currently the network houses over 8000 desktops, 12 campuses and an endless parade of students. His career started in a computer lab support role, through the ranks of Systems Programmers (unofficial security officer), Networks Group Security Officer and is currently the ICT Security Manager.

This institute has enabled him to develop strong technical skills, but also better people skills. He firmly believes people are the biggest hurdle to information security, especially in a tertiary education context where obvious improvements may not be possible when challenged with the concept of academic freedom.

His own challenges to raise information security awareness are ongoing, just like many other Security Officers.

5. References

Australian Government. (2008, April). *Information Privacy Principles under the Privacy Act 1988 - Information Sheet*. Retrieved October 15, 2010, from Office of the Privacy Commissioner: http://www.privacy.gov.au/materials/types/infosheets/view/6541

Australian Government. (n.d.). *National Privacy Principles Plain English Summary*. Retrieved October 15, 2010, from Office of the Privacy Commissioner: http://www.privacy.gov.au/materials/types/law/view/6893

Center for Internet Security. (2010, 08 22). *Center for Internet Security*. Retrieved 08 22, 2010, from Center for Internet Security: http://www.cisecurity.org

Microsoft. (2009, 09 02). *Group Policy Settings Reference for Windows and Windows Server.* Retrieved 09 09, 2010, from Microsoft Download Center: http://go.microsoft.com/fwlink/?LinkId=71758

Stewart James stewart@stootles.com

Office of the Privacy Commissioner. (A). *10 Steps Guide to Protecting Other People's Personal Information*. Retrieved November 30, 2010, from Office of the Privacy Commisioner: http://www.privacy.gov.au/materials/types/guidelines/view/6849

Office of the Privacy Commissioner. (B). *What is Privacy*. Retrieved October 18, 2010, from Office of the Privacy Commissioner: http://www.privacy.gov.au/aboutprivacy/what

Proffit, T. (2008, January 1). *Creating a comprehensive Vulnerability Assessment Program for a Large Company Using Qualysguard.* Retrieved August 22, 2010, from SANS Reading Room: http://www.giac.org/certified_professionals/practicals/GSLC/01376.php

Qualys. (2010a, February). *Qualys Receives Highest Rating in Gartner MarketScope on Vulnerability Assessment*. Retrieved October 15, 2010, from Qualys: http://news.qualys.com/2010/02/qualys-receives-highest-rating.html

Qualys. (2010b, August 22). *QualysGuard*. Retrieved August 22, 2010, from Qualys: http://www.qualys.com/products/qg_suite/

Qualys. (2010c, November). QualysGuard inline documentation.

SANS. (2010a, 08 22). *Audit 507 - Day 1*. Retrieved 08 22, 2010, from SANS Course List: http://www.sans.org/security-training/audit-principles-risk-assessment-effective-reporting-day-1-10342-cid

SANS. (2010b). Auditing Networks, Perimeters, and Systems. *Auditing Networks, Perimeters, and Systems : AUD507.* OnDemand: SANS.

SANS. (2010c). Legal Issues in Information Technology and Information Security. *On Demand.* New York: SANS.

Schneier, B. (2000, April). *The Process of Security*. Retrieved October 18, 2010, from Bruce Schneier: http://www.schneier.com/essay-062.html

Tenable Network Security. (n.d.). *Nessus Professional Feed*. Retrieved October 15, 2010, from Tenable Network Security: http://nessus.org/products/professional-feed/

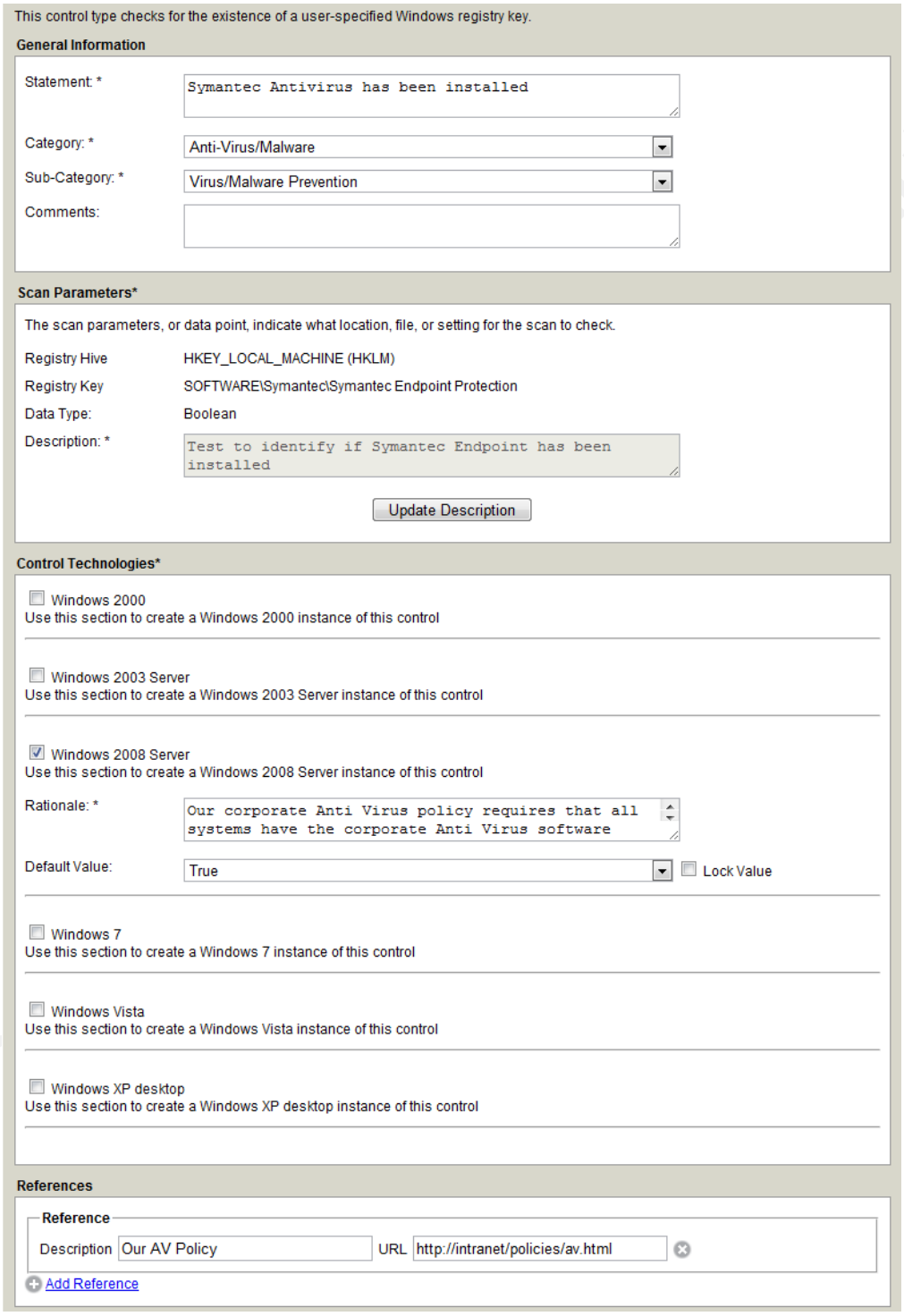
Stewart James stewart@stootles.com

Tenable Security. (2010, 09 09). *Nessus Compliance Checks.* Retrieved 09 09, 2010, from Tenable Security Support Site: https://support.tenablesecurity.com/support-center/nessus_compliance_checks.pdf

Stewart James stewart@stootles.com

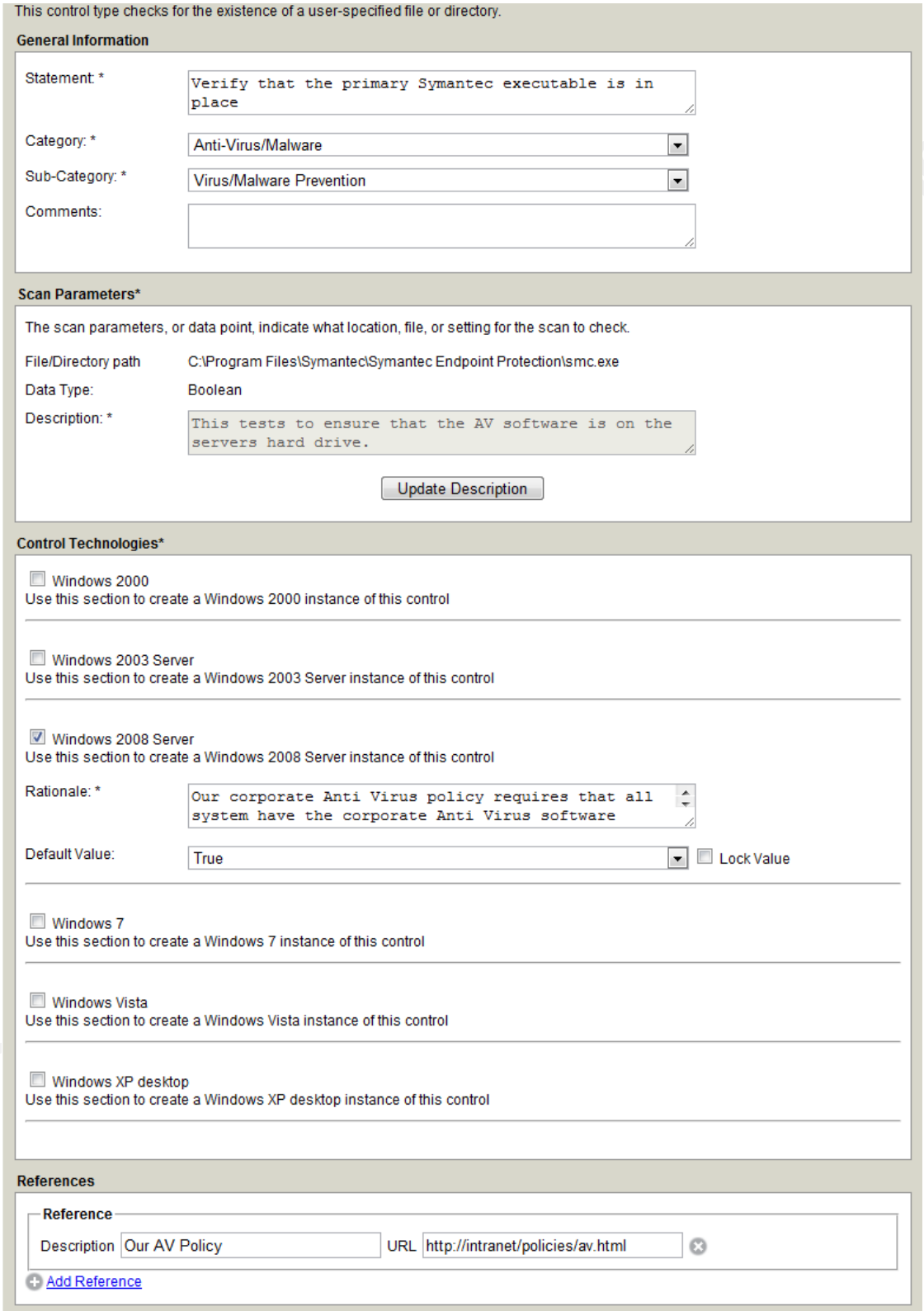
6. Appendix

6.1. Screenshot: Custom rule detecting registry key existence



Stewart James stewart@stootles.com

6.2. Screenshot: Custom rule detecting presence of file



Stewart James stewart@stootles.com