

# QUALYSGUARD® POLICY COMPLIANCE GETTING STARTED GUIDE

April 27, 2012



Copyright 2011-2012 by Qualys, Inc. All Rights Reserved.

Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.  
1600 Bridge Parkway  
Redwood Shores, CA 94065  
1 (650) 801 6100



# Table of Contents

<b>Introducing Policy Compliance .....</b>	<b>5</b>
<b>First Steps .....</b>	<b>8</b>
View Account Info .....	9
View and add compliance hosts .....	10
User roles summary .....	11
Update account settings for sub-accounts .....	12
Add Auditor users .....	14
About the Controls Library .....	14
<b>Policy Management .....</b>	<b>16</b>
About compliance policies .....	16
Creating your first policy .....	18
Step 1: Open the policy editor .....	18
Step 2: Create policy by technology or host .....	19
Step 3: Assign asset groups to the policy .....	21
Step 4: Add controls to the policy .....	22
Step 5: Add more sections to the policy (optional) .....	24
Step 6: Add a cover page (optional) .....	24
Step 7: Save the policy .....	25
Importing a policy from the Library .....	26
Importing a policy from XML .....	27
Add user-defined custom controls .....	28
<b>Compliance Scans .....</b>	<b>31</b>
About compliance scans .....	31
Steps to take before you scan .....	32
Launching compliance scans .....	32
Scan summary notification .....	34
Viewing compliance scans list .....	35
Compliance scan results .....	36
Scheduling compliance scans .....	37
About the Dissolvable Agent .....	38
Detailed Security Auditing for Windows Vista, 7 and 2008 .....	38
Compliance profiles .....	38
Target hosts .....	42
Authentication to hosts .....	42
<b>Compliance Dashboard and Reports .....</b>	<b>44</b>
Dashboard .....	44
Policy Summary .....	45
Compliance Reports .....	46
Run compliance reports .....	46

Authentication Report .....	46
Policy Report .....	48
Control Pass/Fail Report.....	54
Individual Host Compliance Report .....	57
Managing exceptions .....	59
<b>Contact Support.....</b>	<b>61</b>



# Introducing Policy Compliance

QualysGuard<sup>®</sup> Policy Compliance allows customers to audit host configurations and document compliance to internal and external auditors to meet corporate security policies, laws and regulations. This operationalizes Vulnerability Management and Policy Compliance, combining them into a single solution that is delivered as a service, making it easy and cost effective to implement on a global scale.

Policy Compliance is available in your account only when it is enabled for your subscription. If you would like to enable Policy Compliance for your account, please contact Technical Support or your Technical Account Manager.

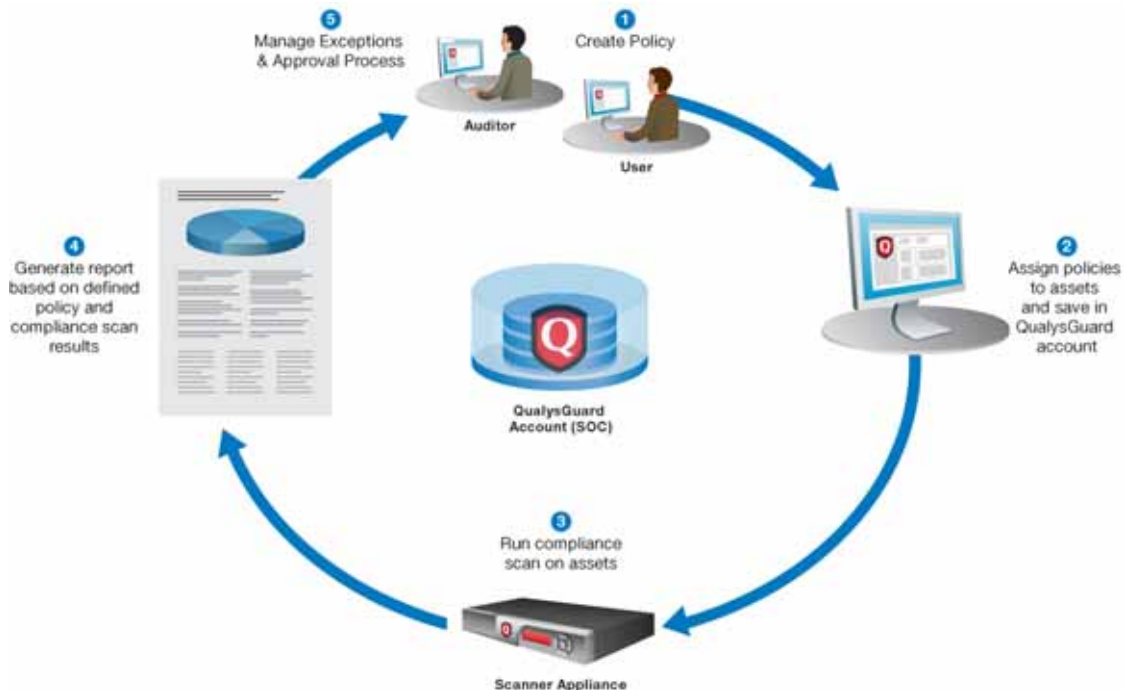
This document introduces QualysGuard Policy Compliance and describes how to get started using QualysGuard Policy Compliance. We will discuss setup requirements, creating and managing policies, performing compliance scans — on demand and scheduled, running compliance reports and managing exceptions. We assume you are familiar with QualysGuard and its vulnerability management features. For information on getting started with QualysGuard, please log into your account and view the online help and the user guides in the Resources section (Help—>Resources).

## Policy Compliance features

- Allows customers to gather compliance and audit data from hosts across the enterprise and measure their configurations against compliance policies and regulations such as SOX, HIPAA, GLBA, CobIT, and ISO17799.
- Compliance scans that leverage the service's authenticated scanning capabilities to read data points from hosts and map them to technical controls defined in compliance policies.
- Policy Compliance workflow that is integrated within the application. Users with compliance management privileges can add compliance hosts, create policies, associate policies to asset groups, run compliance scans, view reports with compliance pass/fail status per policy, host and technical control, create and manage exceptions, and access full audit trail capabilities.
- Auditor user role that grants specific privileges to add custom controls, create policies, approve exceptions, and review policy compliance reports.

## Policy Compliance workflow

The Policy Compliance process is shown below.



### Add Auditor Users (Optional)

Create users with the Auditor user role to perform compliance management tasks. Auditors can create and manage compliance policies for the subscription, generate reports on compliance data and manage exception requests. Auditors are automatically part of the Unassigned business unit and have permission to all compliance hosts defined for the subscription. Note that Auditors only have visibility into compliance data (not vulnerability data).

### Add Custom Controls (Optional)

The service provides technical controls for measuring compliance against a wide variety of technologies, including operating systems (i.e. Windows 2003) and applications (i.e. Oracle 9i). In addition to the service-provided controls, users can add custom controls to the subscription making them available for compliance scanning and reporting. Custom controls are available for Windows and Unix.

These types of custom controls for Windows are available: Registry Key Existence, Registry Value Existence, Registry Value Content Check, Registry Permission, File/Directory Existence, File/Directory Permission and File Integrity Check.

These types of custom controls for Unix are available: File/Directory Existence, File/Directory Permission, File Content Check and File Integrity Check.

## Customize Frameworks for the Subscription (Optional)

When you view technical control information the details include a list of frameworks, standards and regulations that the control maps to. Manager users have the option to customize the list to only display selected frameworks. This setting is made at the subscription level and affects the list of frameworks displayed to all users in technical control information and in policy compliance reports.

## Create Policies and Assign to Relevant Assets

A policy is a collection of controls pertaining to one or more technologies in your environment. Each control in the policy includes a statement of how the technology specific item should be implemented and one or more checks performed by the service to validate the control. After creating a policy, compare the policy to compliance scan results to identify whether hosts are compliant with the policy.

## Run Compliance Scans

Compliance scans identify whether hosts are compliant with user-defined policies. You can launch a compliance scan on hosts that have been defined as compliance hosts for your subscription. Before you launch compliance scans, create compliance profiles and add authentication records for trusted scanning.

**Create compliance profiles.** Users with compliance management privileges can create compliance profiles. Compliance profiles contain scan configuration settings for compliance scans. Note that there are certain scan settings that are automatically set by the service and cannot be edited in a compliance profile. For example, authentication is automatically enabled for all authentication types.

**Add authentication records.** Authentication to hosts is required for compliance scans using QualysGuard's trusted scanning feature. Setup authentication records for all of your compliance scan targets. With authenticated trusted scanning, the scanning engine has the ability to log in to each target host at the time of the scan and obtain in-depth system information.

**Launch compliance scans.** Launch or schedule compliance scans to analyze the policy compliance of your network, using a catalogue of technical controls that is hosted by the service. The technical controls pertain to operating systems and applications, referred to as technologies.

## Generate Compliance Reports

Generate specialized compliance reports on host compliance data. Interactive reports let you change the report source options in real-time to identify the compliance status for individual hosts and the pass/fail status for technical controls. Template-based reports allow you to report on policies in your account, and whether authentication was successful during the most recent scan of each compliance host in your account.

## Manage Exceptions

A workflow is provided for exempting certain hosts from certain controls in a policy. Exceptions are valid until a specified end date as determined by the exception approver. Any user with compliance management privileges can request an exception. Managers and Auditors then review exception requests and either accept or reject them.



## First Steps

When enabled, Managers are granted access to compliance management features automatically. Managers can add Auditor users with access to compliance policy management and reporting features at the enterprise level, without vulnerability management capabilities. Sub-accounts may be added/updated to grant these users role-based access to compliance management.

Title	Type	Created By	Created	Modified By	Modified
My Windows Policy	Compliance	Patrick Stimmer	09/19/2011	Patrick Stimmer	09/19/2011
Dracile Policy	Compliance	Patrick Stimmer	04/20/2010	Patrick Stimmer	09/09/2011
Windows 2003	Compliance	Patrick Stimmer	04/20/2010	Patrick Stimmer	09/09/2011
Windows Share Enumeration	Compliance	Patrick Stimmer	05/02/2011	Patrick Stimmer	09/09/2011
Windows XP	Compliance	Patrick Stimmer	05/05/2011	Patrick Stimmer	09/09/2011
Windows 2000	Compliance	Patrick Stimmer	09/05/2011	Patrick Stimmer	09/09/2011
NY Office	Compliance	Patrick Stimmer	09/09/2011	Patrick Stimmer	09/09/2011
Corporate Office	Compliance	Patrick Stimmer	09/07/2011	Patrick Stimmer	09/07/2011
Policy on Password Management	Compliance	Patrick Stimmer	09/07/2011	Patrick Stimmer	09/07/2011
Locked +8	Compliance	Patrick Stimmer	07/19/2011	Patrick Stimmer	07/19/2011

A. An interactive policy compliance dashboard provides an overall summary of your compliance status across all policies in your account based on compliance scan data in your account.

B. Compliance scans gather compliance data from hosts in asset groups.

C. Compliance reports provide multiple views to review compliance status with a particular policy by business unit, asset group or host. (Note Report Share is enabled.)

D. Exception requests submitted by users. Each request is for hosts/controls in a certain policy. Managers and Auditors may approve exceptions. Unit Managers may approve exceptions when granted this permission.

E. A policy is a written statement of a rule that is applied to operating systems and applications, referred to as technologies, in the network environment.

F. Technical controls based on CIS and NIST standards measure compliance against frameworks and regulations such as COBIT, ISO, ITIL, FFIEC, NERC, etc.

## View Account Info

The Account Info window (Help > Account Info) includes a section called PC Summary. This section displays information about your policy compliance IP addresses, scans, scheduled tasks and pending exceptions. When Managers view this information, they see the total number of compliance IP addresses purchased for the subscription and the total number of compliance IP addresses currently in the subscription.

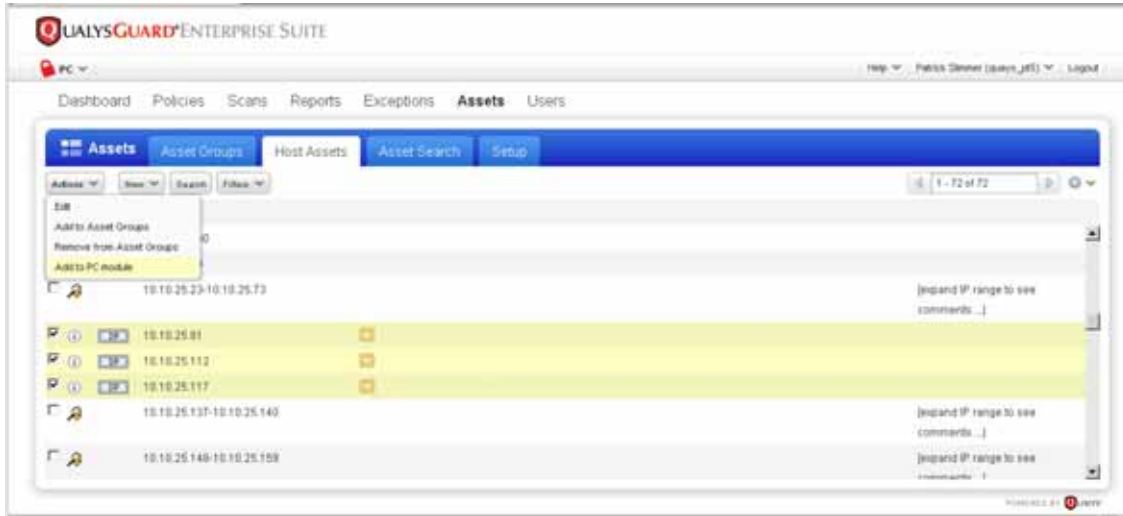


The Account Summary section identifies the applications (modules) that are enabled for your subscription: Vulnerability Management (VM), Payment Card Industry (PCI), and Policy Compliance (PC).



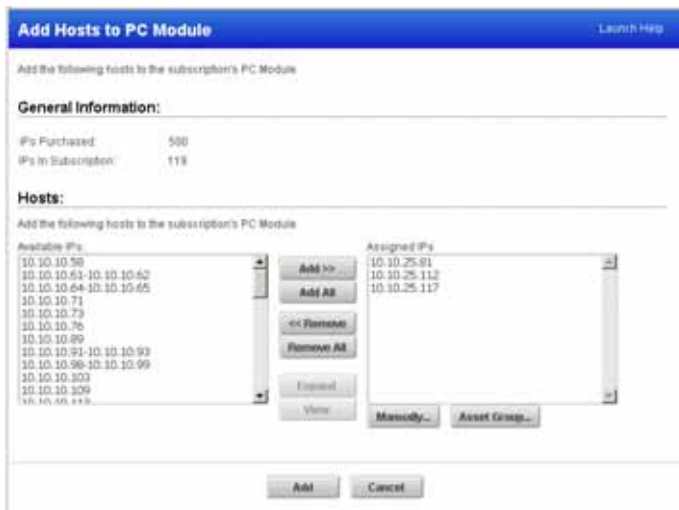
## View and add compliance hosts

The compliance hosts in your account may be selected as target hosts for compliance scanning and reporting. To view the compliance hosts in your account, select Assets from the top menu then click the Host Assets tab. The host assets list appears.



Any host in your account (that is not already in the compliance hosts list) may be added to the Policy Compliance (PC) module, making it available for compliance scanning and reporting. On the host assets list, select the check box next to each host you want to add. You can select individual IP addresses or ranges. Then select Actions > Add to PC module.

The Add Hosts to PC Module wizard appears. The hosts you've selected appear automatically in the Assigned IPs list. You can make changes to this list by adding more IPs to the list or removing IPs from the list. Click Add to add the hosts. Then click OK to confirm the action.



## User roles summary

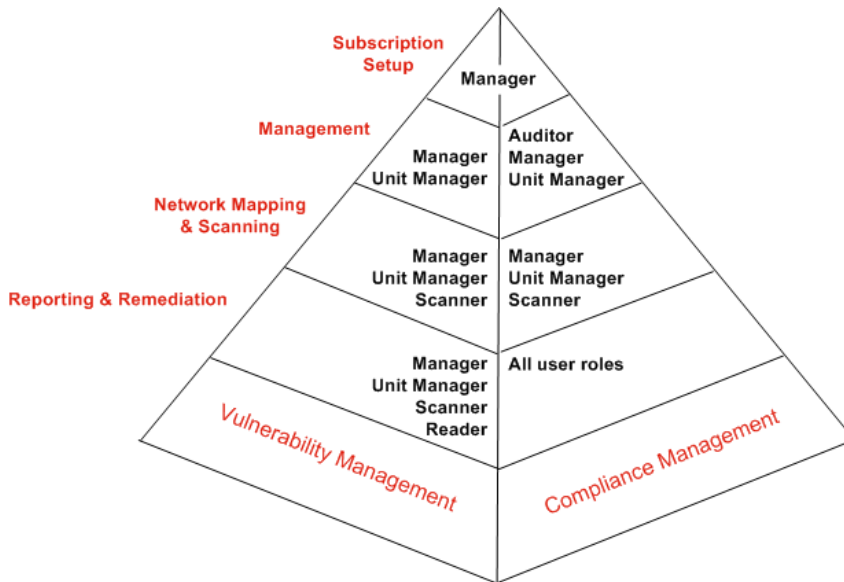
Role-based access controls built into QualysGuard allow multiple users access to the application, with various privileges. Each user account is assigned a user role with certain privileges on their assigned assets (IPs and domains). These user roles may be updated by a Manager or Unit Manager with management authority for the account.

For vulnerability management, these roles are available: Manager, Unit Manager, Scanner, and Reader. All sub-accounts (with user roles except Manager) are granted limited vulnerability management privileges on their assigned assets.

For compliance management, the same user roles for vulnerability management are available plus the Auditor role. The Auditor user role is granted compliance policy management and reporting privileges on all hosts in the subscription. Sub-accounts do not have compliance management privileges, unless the Extended Permission titled “Manage compliance” is enabled in the user’s account settings. When enabled, sub-accounts have limited compliance management privileges on their assigned assets.

Note the following about assigning compliance management privileges. Sub-accounts may be granted compliance management privileges on an individual basis. Managers may grant these privileges to all sub-accounts; and Unit Managers may grant privileges to users in their own business unit. An additional privilege to approve exceptions may be granted to Unit Managers on an individual basis. See “Update account settings for sub-accounts” for further details.

A summary of the QualysGuard user roles for vulnerability management and compliance management is shown below.



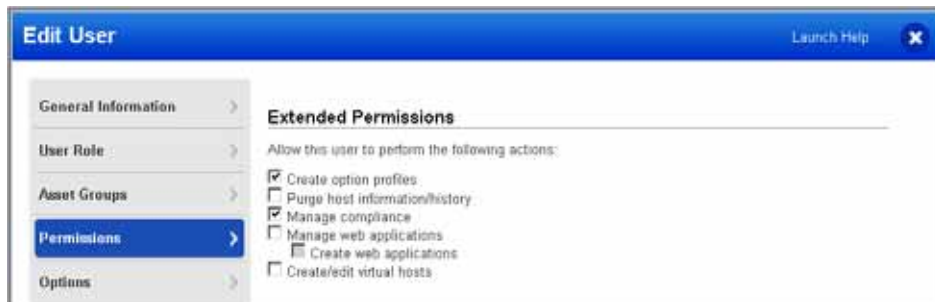
## Update account settings for sub-accounts

For an existing subscription with sub-account users (Unit Managers, Scanners, Readers), Managers should determine which users will participate in compliance management and edit accounts to grant access to this capability, as appropriate.

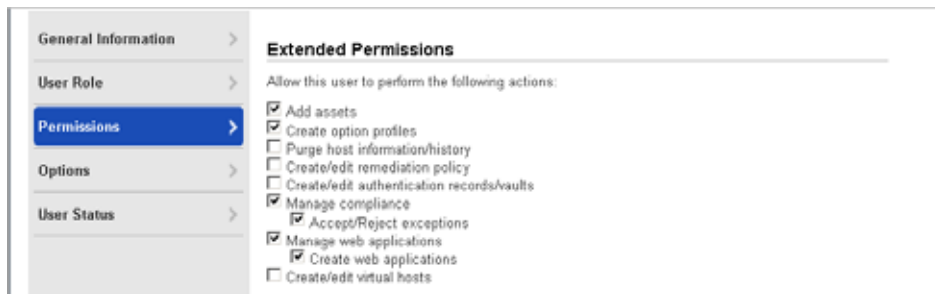
### Set Extended Permissions

Sub-account users will see compliance management functionality when the “Manage compliance” extended permission is enabled in their user accounts. By default, this option is not enabled for sub-accounts. This means existing users cannot access the compliance management features until their user accounts are updated. Managers can edit all sub-accounts in the subscription; and Unit Managers can edit sub-accounts that belong to their business unit.

To edit a user to assign the “Manage compliance” permission, select Users from the top menu and click the Users tab. The user accounts list appears. Edit an account from the list, go to the Permissions section and select “Manage compliance”. Note the list of permissions varies based on the user role. For a Scanner, the permissions list looks like this:



For a Unit Manager, select the permission “Accept/Reject exceptions” to give the user the ability to change the status of exceptions on hosts in their business unit. Select the permission “Add assets” to give the user the ability to add compliance hosts to their business unit, and thus to the subscription. The permissions list for a Unit Manager appears like this:



## Set Notification Options

There are several email notification options available to users. Any user can enable/disable notification options in their own user account settings. Edit your user account, go to the Notification Options section, and select the emails you're interested in receiving. These options are available to users with compliance management privileges:

**Scan Complete Notification** — Select this option to receive an email at the completion of compliance scans (this setting also applies to vulnerability scans).

**Latest Controls** — Select this option to receive an email on a monthly or weekly basis with a list of technical controls that have changed, including new controls that have been added and existing controls that have been modified.

**Exception Notification** — Select this option to receive an email with status changes to policy compliance exceptions that you created and exceptions that have been assigned to you.

For a Manager, the list of notification options appears like this:



## Add Auditor users

Auditors can be added to the subscription by Managers. The Auditor user role:

- Allows Auditors to perform all policy management and compliance reporting functions (not compliance scanning).
- Allows Auditors access to all compliance hosts in the subscription for policy management and compliance reporting functions.
- Does not allow Auditors to perform any vulnerability management functions.

To add an Auditor, select New > User above the user list. Using the wizard, provide general information such as user name and address. continue to the User Role section and select Auditor from the User Role menu. Note: Auditor is automatically assigned the unassigned business unit.



The screenshot shows a web interface titled "New User" with a "Launch Help" button. On the left, there are three tabs: "General Information", "User Role" (which is selected and highlighted in blue), and "Options". The "User Role" section contains the following fields:

- "User Role: \*" with a dropdown menu set to "Auditor".
- "Allow access to:" with two checked checkboxes: "GUI" and "API".
- "Business Unit: \*" with a dropdown menu set to "Unassigned".
- A button labeled "New Business Unit" below the dropdown.


The first time the Auditor logs in they will see the Quick Start with links to compliance management features. An Auditor can create asset groups including compliance hosts, create a policy, create policy report templates and run compliance reports. We will discuss using these features in detail in the sections that follow.

## About the Controls Library

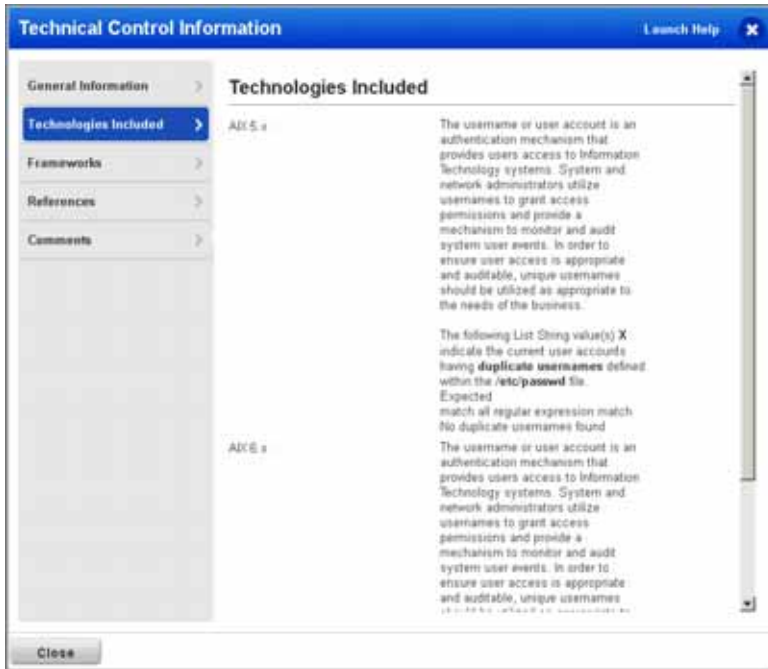
The Controls Library is a centralized location with technical controls for measuring compliance against numerous frameworks and technologies. All controls are based on CIS and NIST standards and map to many frameworks and regulations, such as COBIT, ISO, ITIL, FFIEC, NERC, etc.

To view technical controls, select Policies from the top menu and then click the Controls tab. Controls are classified by category (access control requirements, anti-virus/malware, database settings, etc.) and technology (operating system or application). As appropriate, controls are classified by compliance framework and/or regulatory compliance. The Controls Library is constantly updated, as controls are added and updated by the service.

## View control information

Mouse over a control row and click  (Quick Actions) and select Info to view technical control information. All technical controls include a control statement or title, a CID (control ID), a category and sub-category, and a list of technologies that the control applies to. A control may also be mapped to a list of frameworks, standards and regulations.

For each technology, the control includes a rationale statement, which describes how the control should be implemented for the technology, a description of the data point check to be performed by the scanning engine, and the default expected value for the particular technology. Different technologies can have different default values. (Note that the control in the sample below applies to many more technologies which are not shown in the image.)



## List of frameworks

As stated above, when you view technical control information the details include a list of frameworks, standards and regulations that the control maps to. Manager users have the option to customize the list to only display selected frameworks. This setting is made at the subscription level and affects the list of frameworks displayed to all users in technical control information and in policy compliance reports. To customize the frameworks list, go to Policies and click the Setup tab then select Frameworks. Select the option “Customize list of frameworks” and then select the frameworks you want to display in the subscription.

Additionally, any user with compliance management privileges can customize the list of frameworks in their compliance policy reports. This setting is made in the policy report template.

## User-defined controls

Manager and Auditor users have the option to add user-defined custom controls to the subscription making them available for compliance scanning and reporting in addition to the service-provided controls. Custom controls allow users to create technical policies that better fit their compliance requirements. The service supports various custom controls for Windows and Unix platforms.

See “Add user-defined custom controls” to learn how to add custom controls to the subscription.



# Policy Management

QualysGuard Policy Compliance provides several features and capabilities for policy management and compliance reporting. We recommend that you review the general introduction and then follow the tutorial to create your first policy using the Policy Editor. We'll also describe how to import sample policies into your account from the Policy Library.

## About compliance policies

Let's review the basics about compliance policies and how you manage them in your account.

### Policies

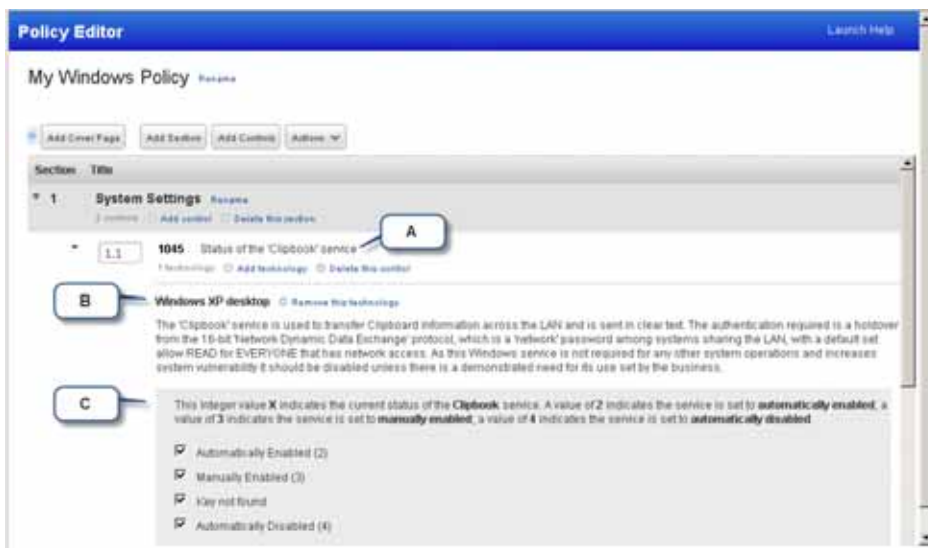
A *compliance policy* is a written statement of a rule that applies to operating systems and applications, referred to as "technologies," in the network environment. You can create multiple policies in your account to check compliance against well-known compliance frameworks, including CobIT, SOX, HIPAA and more. To view your policies, select Policies on the top menu. The policies list will be empty until you (or some user in your subscription) adds a policy.

### Policy Library

A *Policy Library* with several pre-defined, sample compliance policies is included. These policies are based on popular compliance frameworks. See "Importing a policy from the Library."

### Policy Editor

The *Policy Editor* allows you to create and edit policies to test compliance against frameworks. The sample policy below shows control 1045 (A) for the Windows XP desktop technology (B) and the data point value set for the technology (C).



We will walk you through how to create a policy using the Policy Editor in the next few sections. Let's become familiar with the components of a policy, as they appear in the Policy Editor.

### **A. Technical Controls**

*Technical controls* are the building blocks of a compliance policy. When you create a policy you add controls to the policy. The sample Policy Editor screen shows 1 control for the policy titled My Windows Policy. The control appears as an ordered element in the policy. Next to the policy order number, the control ID and statement are shown. The service provides pre-defined controls and users have the option to create custom controls for multiple Windows and Unix technologies.

### **B. Technologies**

A technical control applies to one or more *technologies*, including operating systems such as Windows XP desktop and applications such as Oracle.

When you add a control to a policy, you will notice one or more technologies listed. Some controls apply to multiple technologies and some apply to only one. For each technology, a statement explains the purpose of the compliance check (also referred to as a data point). The technology entries shown in the Policy Editor for a single control will depend on the number of technologies available as well as the technologies included in the policy.

### **C. Data points**

*Data points* are the checks to technologies that validate controls on the policy's hosts. For each control, the service may run one or more compliance checks/data points on the hosts. When creating/editing a policy in the Policy Editor, the service shows a description for each data point. The data point represents a data query comparison to baseline information. For some controls, users may edit the expected value for the data query comparison.

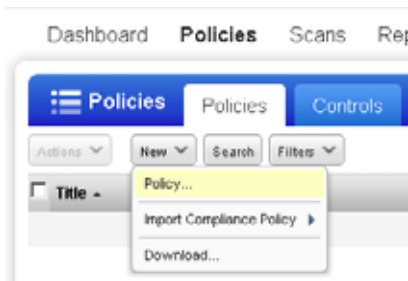
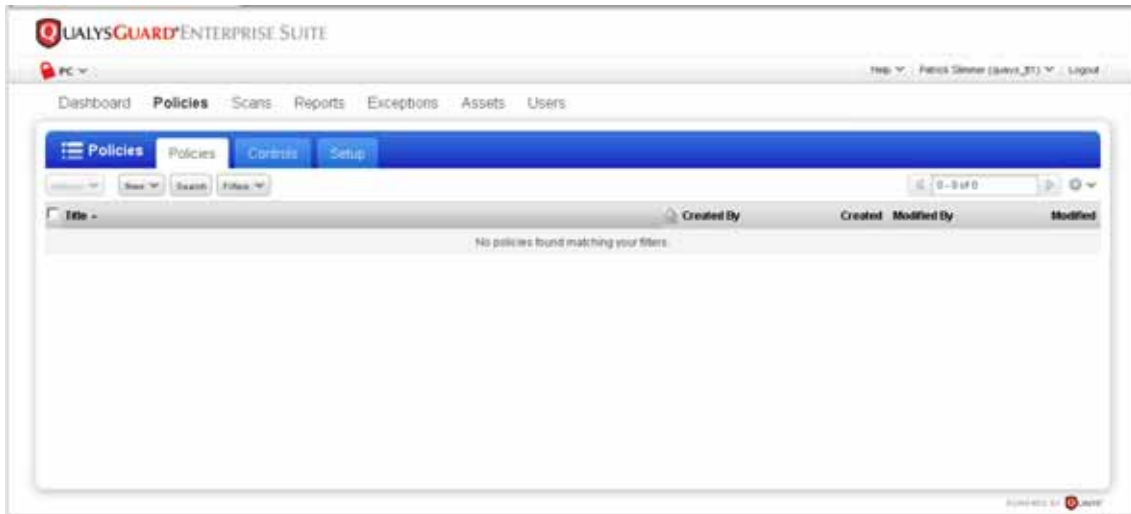
For each data point, the service provides a default expected value. During compliance scans, the service compares the expected value to the actual value returned on each host to determine whether the host is compliant to the control. The compliance reports indicate overall compliance status and status per asset group, host and control. Note that for many data points, like the one shown in the sample policy on the previous page, the service allows you to edit the default expected value and this is reflected in calculating the compliance status in reports. Other data points are locked, meaning that the default expected value cannot be edited.

## Creating your first policy

- Step 1: Open the policy editor
- Step 2: Create policy by technology or host
- Step 3: Assign asset groups to the policy
- Step 4: Add controls to the policy
- Step 5: Add more sections to the policy (optional)
- Step 6: Add a cover page (optional)
- Step 7: Save the policy

### Step 1: Open the policy editor

Select Policies from the top menu then click the Policies tab. The policies list appears. This list is empty until at least one user creates a policy or imports a sample policy.



Go to New > Policy. The Policy Editor appears.

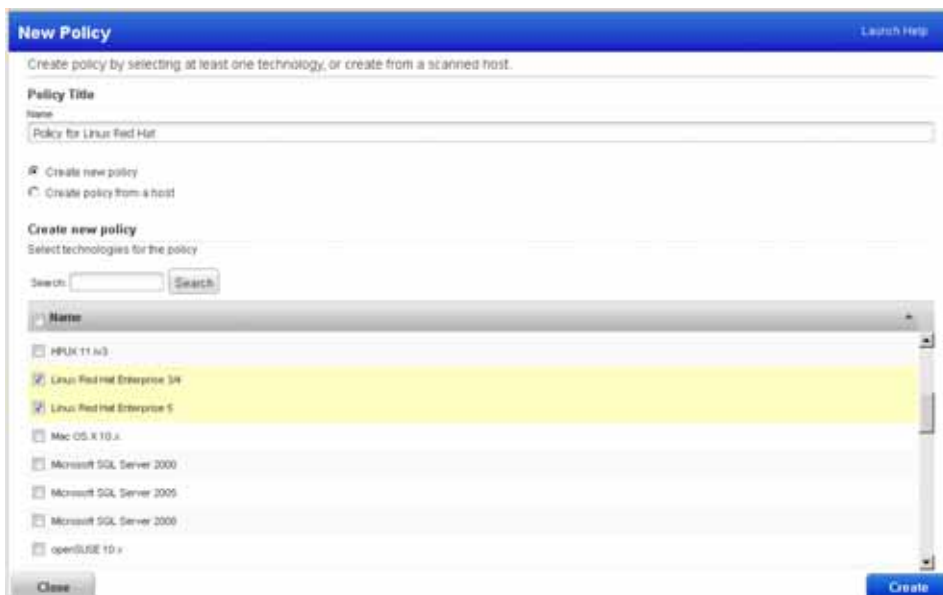
## Step 2: Create policy by technology or host

You are presented with two options for creating the policy: 1) create the policy by first selecting technologies or 2) create the policy by selecting a scanned host to act as a “Golden Image” for the new policy. These options are described in detail below.

### Create a policy by first selecting technologies

This option allows you to create a policy based on technologies that you select. You add controls to the policy based on those technologies. The control values will initially be set to the default values defined by the service for each technology.

In the New Policy window, select the option “Create new policy” (the default). Choose the technologies you want to include in the policy, provide a policy title, and click Create.



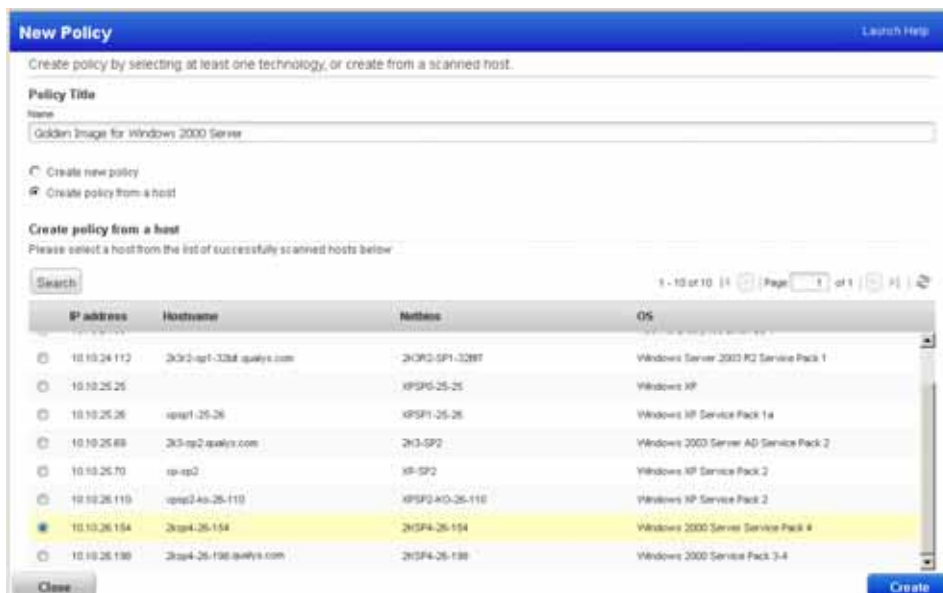
An empty policy is created with the technologies that you selected.



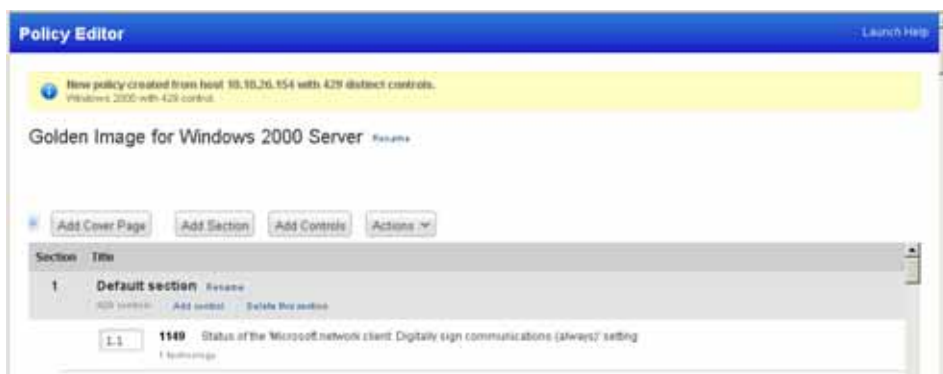
## Create a policy from a host (Golden Image)

The host that you select acts as a “Golden Image” for the new policy. You may select any host that has been scanned for compliance. The service determines which technologies to set for the policy based on the host, and adds controls to the policy applicable to those technologies. Only controls for which there is scan data for the host will be added. The control values are set based on actual values saved in the host scan data.

In the New Policy window, select the option “Create policy from a host”. Select the host you want to base your policy on, provide a policy title, and click Create.



The policy is created with technologies and controls. Note: If multiple scanned instances of a technology are found for the host, then you’ll be prompted to select a single instance to use for the policy. For example, let’s say the host has multiple scanned instances of Oracle 11g on different ports. You’ll need to pick one instance of this technology to continue.



The success message at the top of the page tells you which technologies were added to the policy and how many controls were added for each technology.

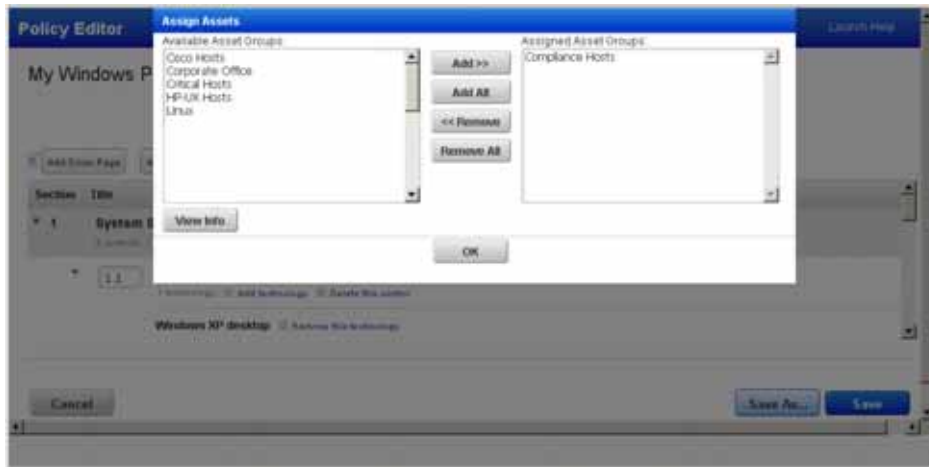
### Step 3: Assign asset groups to the policy

Go to Actions > Assign Assets to assign asset groups to the policy.



In the Assign Assets pop-up, select the groups you want to add and click the Add button. (Optionally, click Add All to assign all of your groups to the policy.) Then click OK.

Assigned asset groups should include hosts that are relevant to the policy. Only the compliance hosts in the assigned asset groups are analyzed for compliance. In the example below, the asset group called Compliance Asset Group is assigned to the policy. When this policy is applied to a compliance report, the compliance hosts in the group will be analyzed.



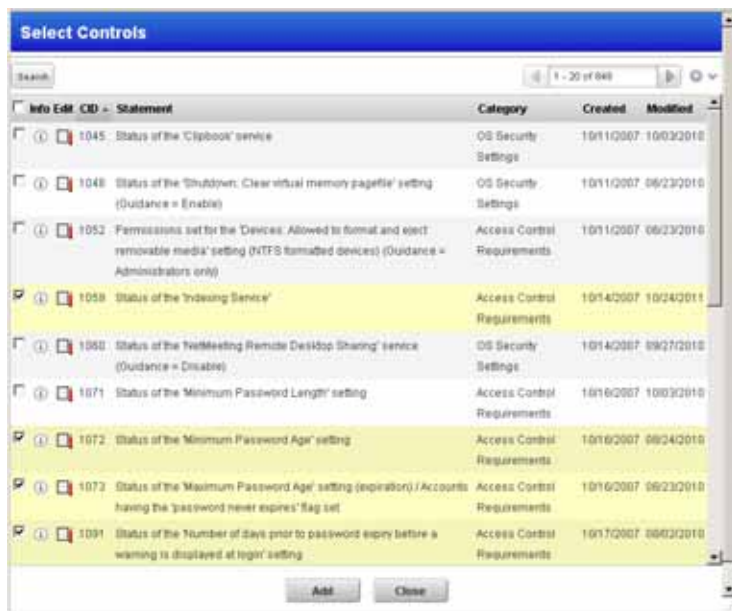
## Step 4: Add controls to the policy

Note: If you created the policy by first selecting technologies, then the policy is empty to start and you must add controls to the policy. If you created the policy by first selecting a host, then controls have been added for you. You may choose to add more controls to the policy.

Click the Add Controls button to add controls that you want to analyze for compliance. You can add as many controls to the policy as you like but may only select up to 200 controls at a time.

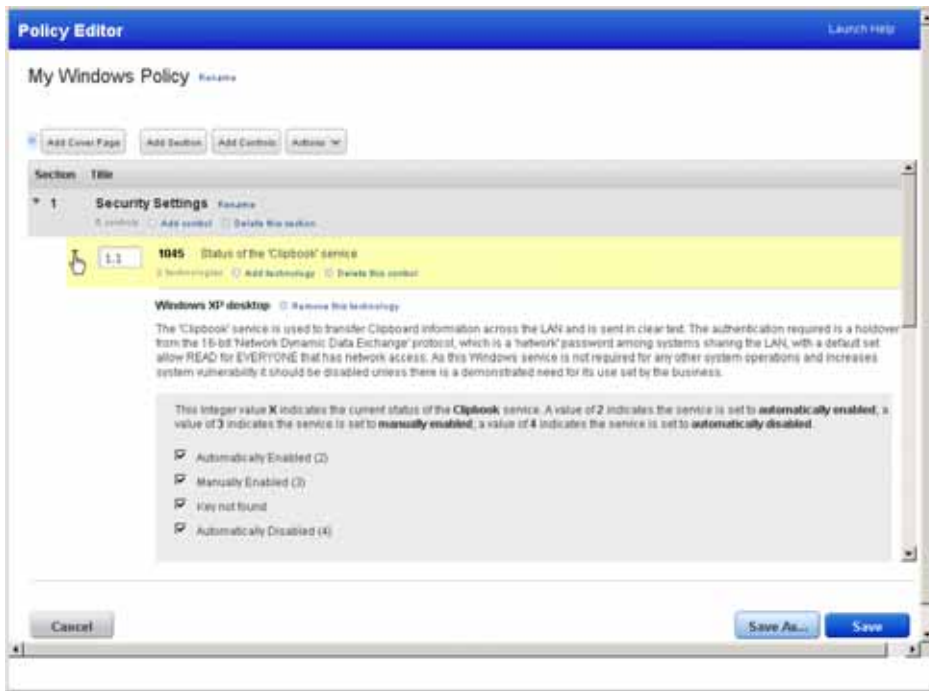


The Select Controls pop-up appears listing controls that you can add to the policy. This list includes controls appropriate to the global technologies list set for the policy. Controls for other technologies not included in the global list are filtered out and cannot be added to the policy.



Select the check boxes for the controls you want to add to the policy, and then click the Add button. The selected controls are automatically added to the last section in the policy.

To expand details for any control in the policy, click that control's row. If a control pertains to more than one technology in the policy, then each technology is listed with a rationale statement relevant to the technology.



See the table below to learn how to work with controls in your policy.

To accomplish this:	Do this:
Add a technology to a control	Mouse over the control and click “Add technology”.
Remove a technology from a control	Click “Remove this technology” next to the technology.
Add/remove a technology for all controls in the policy	Go to Actions > Set Technologies.
Delete a control	Mouse over the control and click “Delete this control”.
Re-order controls	Type over the control number. For example, change control 1.4 to 1.1 to move it up in the section or change control 1.1 to 2.1 to move it from section 1 to section 2.
Set control values	Each control is set to a default value. You can change the value for any unlocked control. You may be required to select an operator (i.e. less than, greater than, equal to), a cardinality (i.e. match any, match all, empty) or both. Then enter the expected value in the field provided. For other controls, you simply select the values (check boxes) that you want to include in the evaluation. Read “Control Values” in the online help for information about the different types of input needed when setting control values.

## Step 5: Add more sections to the policy (optional)

Group controls into sections to provide structure to your policy. For example, you may want to organize controls into sections based on control categories like “Access Control Requirements” and “Database Settings”. Add as many sections as you like and put those sections in any order.

Click the Add Section button to add a new section to the policy. Then provide a title for the section in the pop-up that appears. The new section is added to the end of the policy.



See the table below to learn how to work with sections in your policy.

To accomplish this:	Do this:
Rename a section	Mouse over the section and click “Rename”.
Remove a section	Mouse over the section and click “Delete this section”.
Add a control to the section	Mouse over the section and click “Add control”.
Remove a control from the section	Mouse over the control and click “Delete this control”.
Re-order sections	Click on the section number and enter a new number in the pop-up that appears. For example, change section 3 to section 1 to move it up in the list.
Display an outline view of your policy	Click » on the top left side of the policy. The outline view allows you to quickly jump to a particular control in any section of the policy.

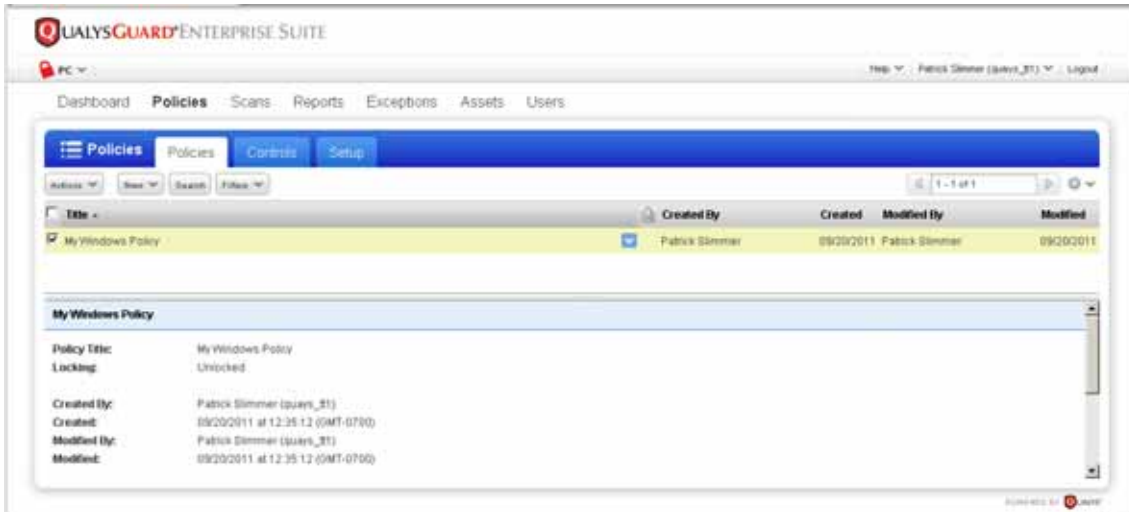
## Step 6: Add a cover page (optional)

Click the Add Cover Page button to add a cover page to the policy. You may want to include a title, date, the name of the user responsible for the policy and your company name and address. The cover page is included when you view and print the policy. It also appears as the first page in policy compliance reports.




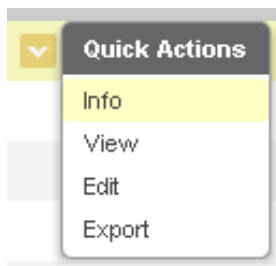
## Step 7: Save the policy

Click the Save button to save the current policy. The saved policy will appear on the policies list. From this list, you can search for policies, view policies, edit policies and delete policies.



Select a policy in the list to display summary information about the policy in the preview pane under the list.

The policies data list allows you to take actions on your policies. Mouse over the policy row and click  and select an action from the Quick Actions menu.



These actions are available:

Info. Select to see policy information.

View. Select to view policy settings.

Edit. Select to make changes to the policy.

Export. Select to export the policy to an XML file.

## Importing a policy from the Library

The service maintains a Compliance Policy Library with several sample compliance policies that you can import directly to your account and use for compliance reporting. These policies are based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Import policies and then assign relevant assets to them.

A gold lock (🔒) next to a policy in the library indicates that the policy is locked. Locked policies may be imported for certification purposes, and they cannot be edited.

Once a policy is imported, you can edit the policy and use the policy in compliance reporting.

To import a sample policy:

- 1 Select Policies from the top menu, and then click the Policies tab.
- 2 Go to New > Import Compliance Policy > Import from Library. The Compliance Policy Library appears.
- 3 Identify the sample policy you're interested in and click the Import button.
- 4 The following status message appears, indicating the sample policy was copied to your account. You are prompted to assign asset groups. It's recommended that you assign asset groups at this time. To do this, click Add Now to assign asset groups. In the Assign Assets window, move asset groups to the Assigned Asset Groups list (see the earlier section "Step 6: Add a cover page (optional)" on page 24) and then click OK.



- 5 If you assigned asset groups to the imported policy, then another status message appears, indicating that the asset groups were added.
- 6 Close the Compliance Policy Library window. The policies list appears with the newly added policy. If you did not assign assets to the imported policy, we recommend that you do so at this time. Only hosts in assigned asset groups are analyzed for compliance. To assign assets to a policy, edit the imported sample policy, and then add asset groups to the policy in the Policy Editor window.

## Importing a policy from XML

Import a policy directly into your account from an XML file. The XML file may be one that was exported from your account or one that was shared with you by another security professional. Once imported, the policy appears in your policies list where you can assign asset groups to the policy and customize the policy settings.

To import a policy from an XML file:

- 1 Select Policies from the top menu, and then click the Policies tab.
- 2 Go to New > Import Compliance Policy > Import from XML file.
- 3 Provide a title for the imported policy, and then browse to the policy XML file.

- 4 Click Import.
- 5 When the Success message appears, do one of the following: 1) Click Open Policy to immediately view the policy in the Policy Editor where you can assign asset groups to the policy and customize the policy settings. 2) Click Close to close the Success message and return to your policies list.

### How It Works

When you import a policy from an XML file, the service performs several validation checks on the XML. If validation is successful, the policy is saved to your policies list. If validation fails, an error appears and the policy cannot be imported. Fix the XML and try again.

If the <EVALUATE> tag is present for any control, its checksum is validated to ensure that the evaluation logic hasn't been modified since the policy was exported. If the evaluation logic has changed then validation will fail. Note that you may remove the <EVALUATE> tag for any control. When the <EVALUATE> tag is not present for a control, the control is automatically assigned the default control value from the controls library.

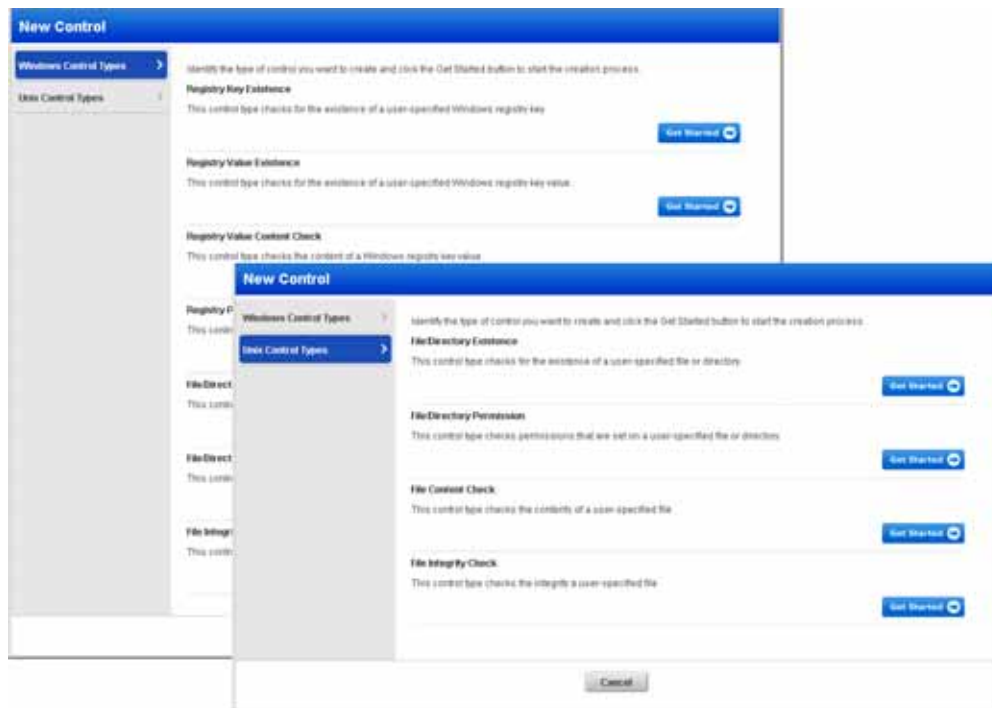
## Add user-defined custom controls

Managers and Auditors have the option to add user-defined custom controls to the subscription making them available for compliance scanning and reporting. The service supports custom controls for both Windows and Unix platforms.

When defining a custom control, you must 1) provide general information for the control like a control statement and category, 2) specify the scan parameters that define the data point check to be performed by the scanning engine, and 3) identify the technologies that the control applies to and set the default expected value for each technology.

To add a custom control:

- 1 Select Policies from the top menu, and then click the Controls tab.
- 2 Go to New > Control.
- 3 In the New Control window, select Windows Control Types or Unix Control Types.



- 4 Identify the type of control you want to create and click the Get Started button.
- 5 Provide details in the following sections: General Information, Scan Parameters, Control Technologies and References. (See the online help for complete information.)
- 6 Click Create to save the new control.

Once saved, the custom control appears in the controls list with the service-provided controls. The service automatically assigns the new custom control a unique CID (Control ID) starting at 100000. Subsequent CIDs are incremented by one — 100001, 100002, 100003, etc. The new control is automatically included in all future compliance scans and may be added to policies.

## Sample Control: Unix File Content Check

A Unix File Content Check control checks the contents of a user-specified file on a Unix system.

A Unix File Content Check control includes 2 regular expressions. The first regular expression is entered in the Scan Parameters section and is used to filter results on the target file/directory at the time of the scan. The second regular expression is entered as the default value in the Control Technologies section and is used to perform the pass/fail evaluation of the returned results.

### Example:

This sample control can be used to find lines in the `/etc/passwd` file that end with `/bin/bash`.

The settings in the Scan Parameters section instruct the scanning engine to first return all lines in the `/etc/passwd` file that have at least one character. The settings in the Control Technologies section instruct the scanning engine to pass the control if none of the lines end with `/bin/bash`. If at least one line in the file ends with `/bin/bash` then the control will fail.

**New Control: File Content Check** Launch Help

This control type checks the contents of a user-specified file.

**General Information**

Statement \*

Category \*

Sub-Category \*

Comments

**Scan Parameters\***

The scan parameters, or data point, indicate what location, file, or setting for the scan to check.

File path \*

Regular expression \*

Data Type

Description \*

**Control Technologies\***

AdX 5.x  
Use this section to create a AdX 5.x instance of this control.

Rationale \*

Cardinality \*   Lock Cardinality

Operator \*   Lock Operator

Default Value   Lock Value

## Sample Control: Windows Registry Permission

A Windows Registry Permission control checks permissions that are set on a Windows registry key for different user groups and individual users.

To maximize space, the Policy Compliance application assigns each permission a letter (A,B,C,D,...) and displays the letter instead of the full permission name. You must use the same mapping when setting the default expected value for the control. (See "Registry Permissions" in the online help for a table that maps each permission to the letter it represents.)

### Example:

This sample control checks that the registry key HKLM\SYSTEM has the following permissions:

The Administrators group has Full Control permission (D:E:F:G:H:I:J:K:L:M)

The Users group has Read permission (E:F:I:M)

A user named Robert has Read Control permission (M)

**New Control: Registry Permission** Cancel Help

This control type checks permissions that are set on a Windows registry key.

**General Information**

Statement \*

Category \*

Sub-Category \*

Comments:

**Scan Parameters\***

The scan parameters, or data point, indicate what location, file, or setting for the scan to check.

Registry Hive \*

Registry Key \*

Data Type:

Description \*

**Control Technologies\***

Windows 2000  
Use this section to create a Windows 2000 instance of this control.

Rationale \*

Cardinality \*   Lock Cardinality

Operator \*   Lock Operator

Default Value:   Lock Value



# Compliance Scans

Users with scanning privileges can launch and schedule compliance scans and view scan results, much like they launch/schedule vulnerability scans. Users with scanning privileges include Managers, Unit Managers and Scanners; Auditors do not have scanning privileges. Please note that authentication to target hosts is required for compliance scans. If authentication records for target hosts do not exist, you must create them before running compliance scans.

## About compliance scans

Compliance Scans analyze the policy compliance of your network, using the Controls Library that is hosted by the service. The technical controls pertain to operating systems and applications, referred to as technologies, which are the building blocks for compliance policies. Successful authentication to hosts is essential for obtaining in-depth compliance data used for policy compliance analysis.

The service scans for all technical controls including controls that have not yet been added to a policy. You have the option to restrict the scan to controls in a specific policy that you choose in the compliance profile. See “Compliance profiles.”

When you launch or schedule compliance scans, the service safely and accurately measures compliance against the available technical controls using its Inference-Based Scanning Engine, an adaptive process that intelligently runs only tests applicable to each host scanned. The impact of scans on your network load is minimal because the service samples your available bandwidth and then uses a fixed amount of resources.

Each control may apply to one or more technologies and may include one or more individual compliance checks. For this reason, it's best practice to schedule network security audits and compliance reports regularly to minimize potential risk and ensure constant compliance. We recommend scheduling routine weekly scans plus running a manual on-demand scan whenever new network devices are introduced or configurations are updated.

## External and Internal Scanning

External scanning at the network perimeter is available to all users (with scanning privileges) using the external scanners. Internal scanning of private use internal IPs is supported using scanner appliances, installed inside the corporate network. With scanner appliances you have more scanner options to apply to each scan task. You may select a scanner appliance to send the scan task to a particular appliance, or you may select the scanner parallelization option to distribute the scan task across multiple scanners and thus improve scan performance.

There are several events that take place during the compliance scanning process: Host Discovery, Port Scanning, Operating System Detection, Service Discovery and Compliance Assessment. For more information, see “How does Compliance Scanning Work” in the QualysGuard online help.

## Steps to take before you scan

Before you launch or schedule compliance scans, follow these steps to ensure your scans are successful and you get the most out of your scans:

### Step 1: Accept the Dissolvable Agent

A Manager must accept the Dissolvable Agent (Agent) in order to run certain compliance scans to test for Password Auditing, Windows Share Enumeration and/or Detailed Security Auditing for Windows Vista, 7 and 2008. See “About the Dissolvable Agent.”

### Step 2: Create compliance profiles

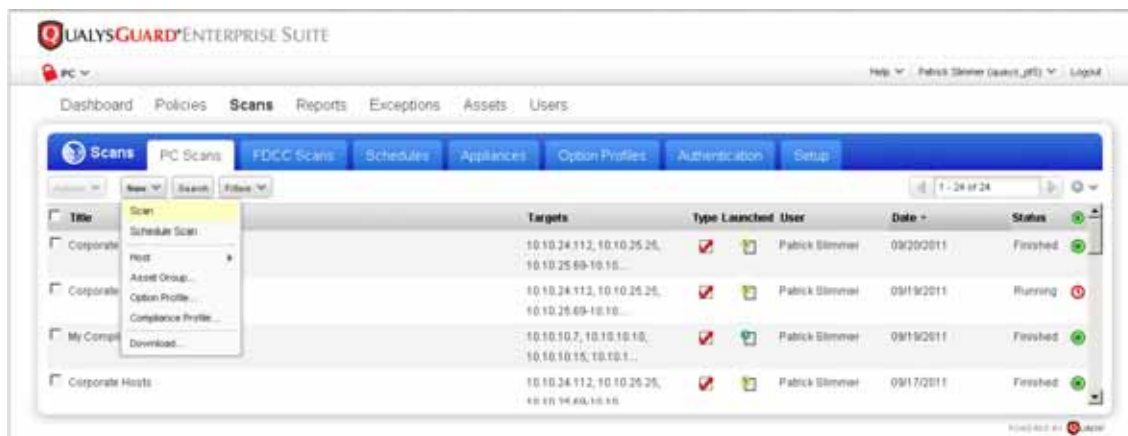
Compliance profiles contain scan configuration settings. Before you can launch a compliance scan, a compliance profile must be available on the option profiles list in your account. The service does not provide a default compliance profile. A Manager or another user with compliance management privileges can create a compliance profile. See “Compliance profiles.”

### Step 3: Add authentication records

Successful authentication to target hosts is a requirement for compliance scans. Authentication records identify credentials used to authenticate to target hosts during scans. If authentication to a host is not successful, then no controls can be evaluated for the host and no compliance data can be collected for the host. If authentication to a host is successful, then the host can be evaluated for compliance. See “Authentication to hosts.”

## Launching compliance scans

Compliance scans can be launched on demand and scheduled to run at a future date and time. To launch an on-demand scan, select Scans from the top menu and click the PC Scans tab. The compliance scans list appears. Go to New > Scan.



The Launch Scan wizard appears, prompting you to enter scan information.

**Title** — The title helps you identify the scan within the application. The title you enter appears in the scan summary email and the scan results report.

**Compliance Profile** — Select a compliance profile to apply to the task from the menu. The profile identifies scan settings. This menu is empty until you (or another user in your subscription) creates a compliance profile. See “Compliance profiles.”

**Scanner Appliance** — When your account has scanner appliances, select a scanner option from the menu: External, scanner appliance name, All Scanners in Asset Group, or Default. (These same options are available for vulnerability scans.)

**Target Hosts** — Select compliance IPs/Ranges and/or asset groups with compliance hosts. See “Target hosts.” Authentication to target hosts is required for compliance scans. Be sure that all target hosts are defined in authentication records in your account. See “Authentication to hosts”.

After entering information, click the Launch button. The scan status will appear, as shown below:

The Scan Status report is updated every 60 seconds until all targeted hosts have been analyzed, allowing you to view results in real time. The current status is listed as “Running” when a scan is in progress. Once the scan finishes analyzing all target hosts, the current status is listed as “Finished”, as shown below:

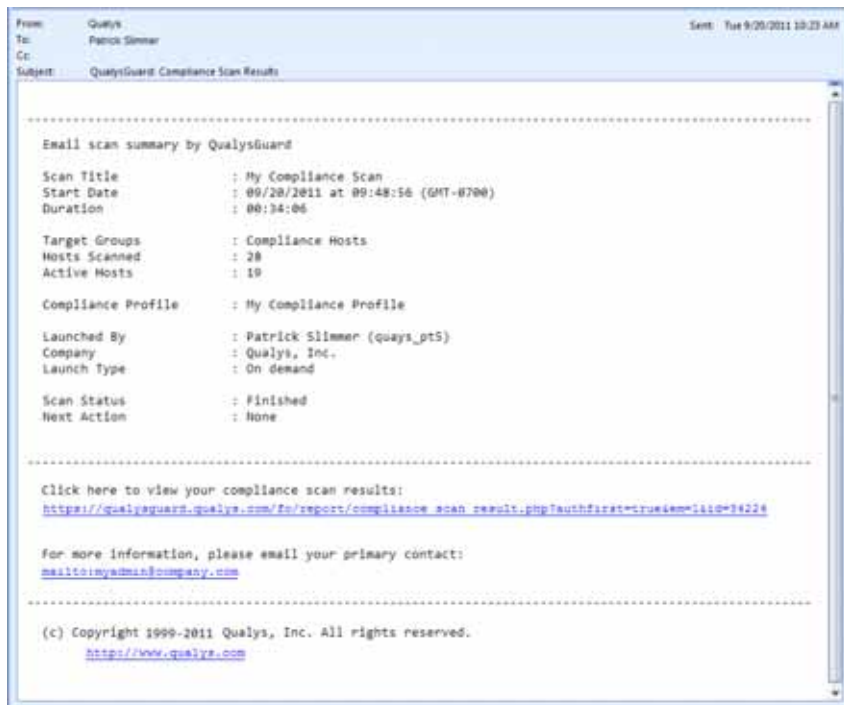


Note the scan status for a compliance scan (unlike the scan status for a vulnerability scan) does not show a summary for each successfully scanned host. The scan task runs in the background, so you can close the status window and view the scan status by going to the scan history list (see "Viewing compliance scans list").

## Scan summary notification

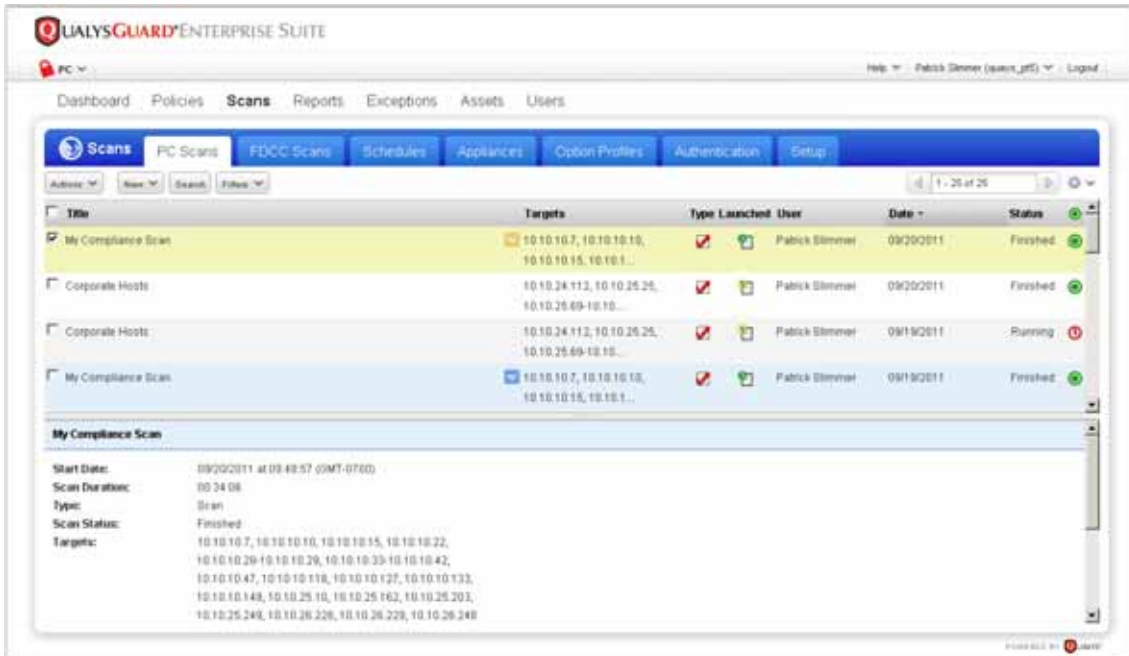
A scan email notification is sent at the completion of compliance scans when the Scan Notification option is enabled in your account. This setting applies to both vulnerability scans and compliance scans. Any user can edit their own account to enable/disable this setting.

A sample notification for a compliance scan is below.



## Viewing compliance scans list

The compliance scans list shows compliance scans that are running and finished. To view this list, go to Scans and click the PC Scans tab.



You'll notice the Type column shows the scan type: for compliance scan. The Status column indicates whether the scan is Running or Finished.

### Perform actions on scans:

Mouse over a scan row and click (Quick Actions) and select one of these actions:

View. View the current scan status (running scans) or compliance scan results (finished scans).

Download. Download compliance scan results to one of these file formats: PDF, HTML, MHT, XML or CSV.

Relaunch. Relaunch a previous scan. The service makes a best effort to recall the previous scan's settings and prefill values as a convenience. The current date is appended to the previous scan's title for quick identification.

Pause/Resume. Pause and resume a running scan. A paused scan must be resumed within 30 days from the initial launch date, otherwise it will be canceled automatically.

Cancel. Cancel a running scan.

To delete a scan select the scan and then select Actions > Delete.

## Compliance scan results

Sample scan results are below. The Report Summary provides information about the scan.



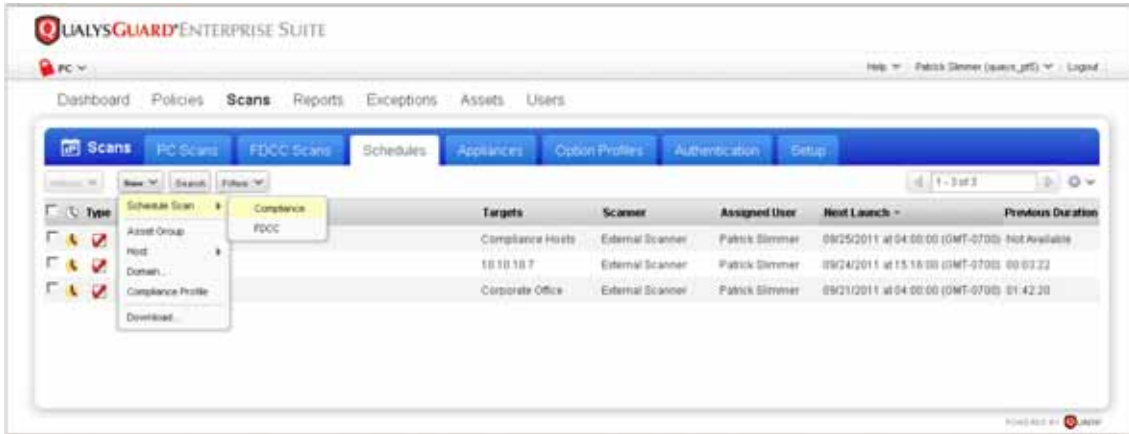
The Appendix lists hosts scanned/not scanned, authentication status for compliance hosts by authentication type, and compliance profile settings (not shown).



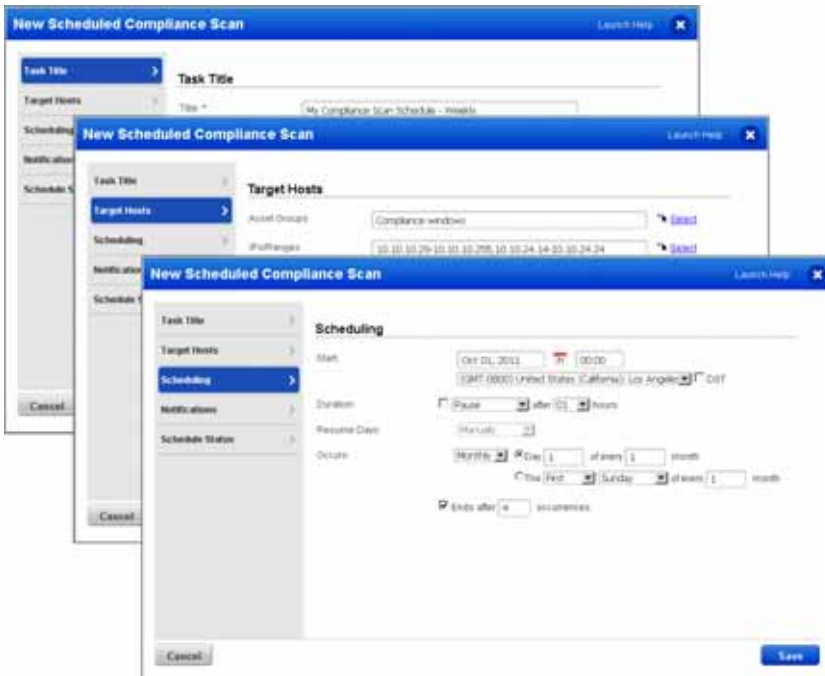
To identify whether hosts are compliant with user-defined policies, generate specialized compliance reports (template based and interactive) based on compliance scan data. See "Compliance Dashboard and Reports" for complete information.

## Scheduling compliance scans

You can define schedules for compliance scans, just as you can for vulnerability scans. Select Scans from the top menu and click the Schedules tab. Go to New > Schedule Scan > Compliance.



The New Scheduled Compliance Scan wizard appears where you can add the task. You'll notice the schedule settings are similar to a vulnerability scan schedule, except you enter a compliance profile instead of an option profile.



## About the Dissolvable Agent

The Dissolvable Agent (Agent) is installed on Windows devices to collect host data in order to perform certain compliance scans. During the scan process the Agent is installed as needed. Once the scan is complete, the Agent will remove itself completely.

Information collected by the Agent is securely transmitted to the scanner using a cryptographically secure protocol. The information is encrypted and integrity-protected and is not stored on the scanner except in memory while the information is processed. The information is discarded securely as soon as it is no longer needed.

Agent installation is required for these capabilities: Password Auditing (enable in the compliance profile), Windows Share Enumeration (enable in the compliance profile), and Detailed Security Auditing for Windows Vista, 7 and 2008 (no profile changes needed).

### Accept the Agent (Manager Only)

Any Manager user can accept the Dissolvable Agent for the subscription. To accept the Agent, Select Scans from the top menu and click the Setup tab, then select Dissolvable Agent. Review the Agent installation status, if any, and then click the Accept button.

## Detailed Security Auditing for Windows Vista, 7 and 2008

Detailed Security Auditing for Windows Vista, 7 and 2008 enables you to run compliance scans to test detailed security auditing settings, per the latest security guidelines from CIS and Microsoft.

To perform these security tests, a Manager must accept the Dissolvable Agent (Agent) for the subscription. There are 53 security auditing tests included. Please note these security tests will be performed automatically by the service once the Agent is accepted, without changes to your compliance profile. See "Detailed Security Auditing for Windows Vista, 7 and 2008" in the online help for a list of the security auditing tests.

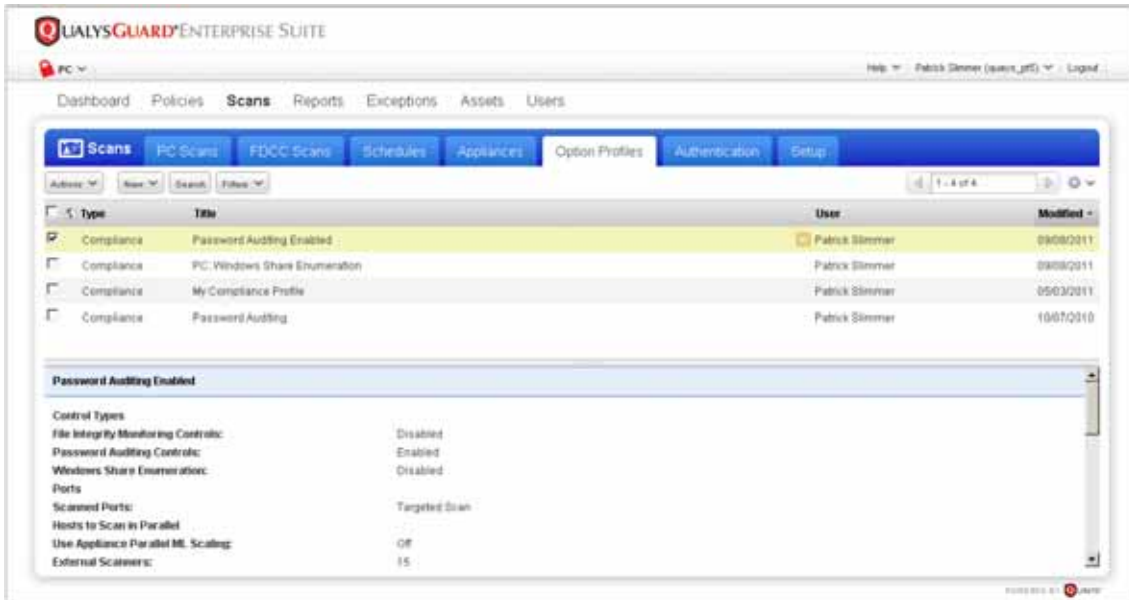
## Compliance profiles

When you launch or schedule a compliance scan, you'll be required to select a compliance profile to apply to the task. Note the service does not provide default compliance profiles. Before you launch a compliance scan, you (or another user in your subscription) must create a compliance profile to apply to the scan.

User Permissions: Managers can create compliance profiles. Unit Managers and scanners must be granted this permission. Managers can edit any profile, regardless of owner. Unit Managers can edit any profile that they created for personal use and profiles created by other users in their business unit. Scanners can edit only those profiles that they created for personal use.

### View compliance profiles

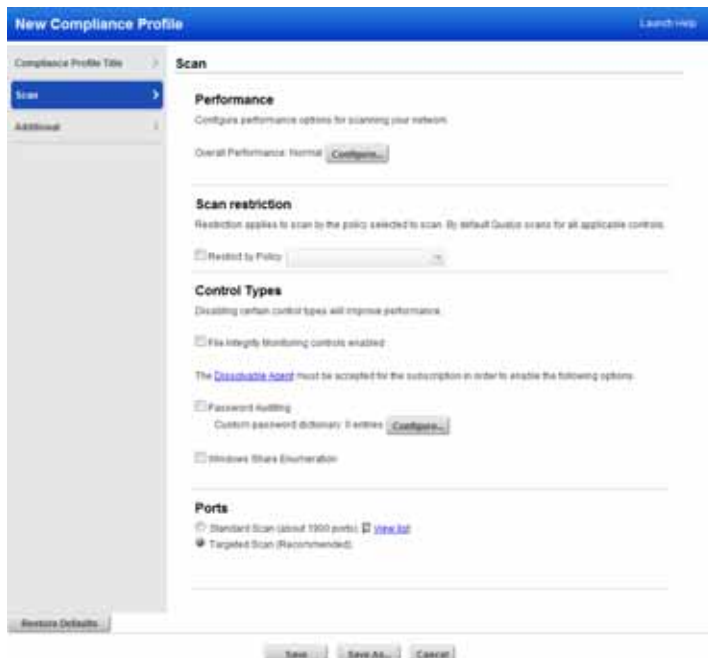
To view the compliance profiles in your account, select Scans from the top menu and click the Option Profiles tab. When the Policy Compliance application (module) is first enabled for your account, there are no compliance profiles listed until you (or another user in your subscription) adds one.



## Add a compliance profile

To add a compliance profile, go to New > Compliance Profile. Below you'll see a sample compliance profile with initial settings provided by the service.

The Scan section of the compliance profile includes configuration settings that affect how the service gathers information about target hosts and how the service performs compliance assessment on target hosts.



Scan options include:

**Performance** — The overall performance level is High, Normal, Low or Custom. The performance level determines the number of hosts to scan in parallel, the number of processes to run in parallel against each host, and the delay between groups of packets sent to each host. Click **Configure** to change the overall performance level or customize performance settings.

**Scan restriction** — This option allows you to restrict the scan to a specific policy. When selected, the service will only scan for the controls in the selected policy. If you add new controls to the policy, be sure to launch another scan to collect scan data for the new controls. When not selected, the service will scan for all controls including controls that have not yet been added to a policy.

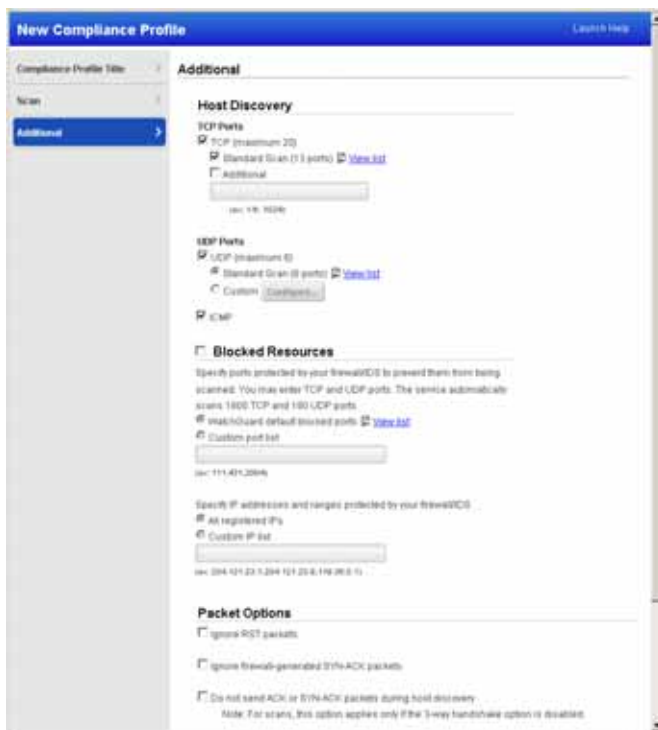
**Control Types: File Integrity Monitoring controls enabled** — This option allows you to monitor changes to individual files on your network. To use this option, you must define custom File Integrity Check controls that identify the files you want to monitor for changes. See “File Integrity Monitoring” in the online help for step-by-step instructions.

**Control Types: Password Auditing** — This option allows you to perform password auditing. When enabled, the scan checks for 3 service-provided password auditing controls that identify user accounts 1) with empty passwords, 2) with the password equal to the user name, and 3) with passwords equal to an entry in a user-defined password dictionary. Note this option can only be enabled if the Dissolvable Agent has been accepted for the subscription. See “Password Auditing” in the online help for step-by-step instructions.

**Control Types: Windows Share Enumeration** — This option allows you to check Windows shares that are readable by Everyone and return the number of files for each share on the host. Note this option can only be enabled if the Dissolvable Agent has been accepted for the subscription. See “Windows Share Enumeration” in the online help for step-by-step instructions.

**Ports** — (Applies to Unix and Windows scans only) Define the ports to be scanned. When “Standard Scan” is selected, the standard ports (about 1900 ports) are used, including the well known ports: 22 (SSH), 23 (telnet) and 513 (rlogin). For Unix hosts, any custom ports specified in the Unix authentication record are also scanned. When “Targeted Scan” is selected, the service targets the scan to a smaller set of ports than the standard ports. This is the recommended setting, and it is the initial setting for a new compliance profile.

The Additional section of the compliance profile includes configuration settings that affect how the service performs host discovery and how the service interacts with your firewall/IDS configuration. The initial settings are best practice in most cases. These settings should be customized only under special circumstances.



Additional options include:

**Host Discovery** — Specify which probes are sent and which ports are scanned during host discovery. The service pings every target host using ICMP, TCP, and UDP probes and then analyzes the packets sent in response to determine which hosts are “alive”. Important: By changing the default settings, the service may not detect all live hosts and hosts that go undetected cannot be scanned.

**Blocked Resources** — Specify ports that are blocked and IP addresses that are protected by your firewall/IDS. If the scanning process triggers your IDS, then it will likely be firewalled and we won’t be able to continue our search for compliance data. Therefore, we need to know which IPs you have protected and which ports are blocked. This will help us prevent triggering your IDS.

**Packet Options** — Specify certain types of packets to ignore, including TCP Reset packets and TCP SYN-ACK packets that appear to originate from a filtering device. You can also suppress the service from sending out of state ACK and SYN-ACK packets during host discovery.

## Target hosts

Target hosts for compliance scans must be defined in your account as compliance hosts. See “View and add compliance hosts” for assistance with identifying the compliance hosts in your account.

Compliance hosts are the targets for compliance scans. Typically, compliance hosts consist of a sub-set of the host assets in the subscription. Other host assets are targets for vulnerability scans and reports. Each host in the subscription is tracked by IP address initially but you can change the tracking method to DNS hostname or NetBIOS hostname.

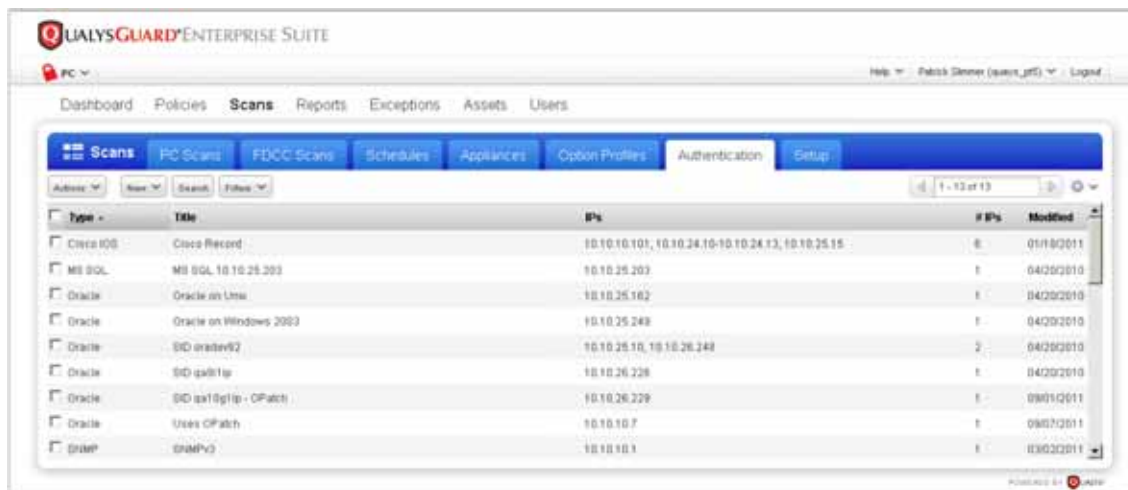
You have the option to specify asset groups as targets for compliance scans, limiting the scope of the scan and making the results more manageable. Asset groups may have a combination of standard hosts, which may be targets for vulnerability scans, and compliance hosts, which may be targets for compliance scans. When an asset group contains standard hosts and compliance hosts, only the compliance hosts are scanned.

## Authentication to hosts

Authentication to hosts is required for compliance scans using QualysGuard’s trusted scanning feature. For Windows compliance scanning, an account with Administrator rights is required; a compliance scan fails and does not return scan results if an account with less privileges is used.

The service performs authentication based on authentication records you define for your target hosts. Each authentication record identifies an authentication type — Windows, MS SQL Server, Unix, Oracle, SNMP or IBM DB2 — account login credentials and target IP addresses. Multiple records may be defined. The service uses all the records in your account for compliance scanning.

To view authentication records in your account, select Scans from the top menu and click the Authentication tab.



To add authentication records, go to the New menu above the list and select a record type. The online help describes each record type and the required login credentials.

Tips:

No data found — If you run a compliance scan and it returns the status “Finished” with the message “No data found” it’s most likely that authentication was not successful on the target hosts. Be sure to create authentication records for the systems you want to scan. Also check that the credentials in the records are current.

Authentication Report — The Authentication Report helps you identify where authentication was successful and where it failed for compliance hosts. For each host, authentication status Passed, Failed or Passed with Insufficient Privileges (Passed\*) is provided. See “Authentication Report” for more information.

## Special Settings in Authentication Records

### Oracle — Allow scanning multiple instances (SIDs) on IPs/ports also used in other records

Select this option in your Oracle authentication record to perform compliance scans on multiple instances (SIDs) running on host and port combinations in the record. This option must be selected if the Oracle record has some host and port combination, which is already defined in another record. When selected, this record will be used for compliance scans only (not vulnerability scans).

### Oracle — Perform OS-dependent compliance checks

Select this option in your Oracle authentication record and provide details about your Oracle installation to allow the scanning engine to gather Oracle compliance data at the operating system level. (Important: Hosts defined in an Oracle record must also be defined in a Windows record or a Unix record.)

### IBM DB2 — Perform OS-dependent compliance checks

Select this option in your IBM DB2 authentication record and provide details about your IBM DB2 installation to allow the scanning engine to gather IBM DB2 compliance data at the operating system level. (Important: Hosts defined in an IBM DB2 record must also be defined in a Windows record or a Unix record.)

### Unix — Custom Ports

The scanning engine needs to find login services in order to successfully authenticate to Unix hosts and perform compliance assessment. If services (SSH, telnet, rlogin) are not running on well known ports (22, 23, 513 respectively) for the hosts you will be scanning, then you must define a custom ports list in your Unix authentication record.

## Use of Authentication Vaults (optional)

The service supports the use of these vaults for authenticated scanning of Windows and Unix hosts: Cyber-Ark PIM Suite and Thycotic Secret Server..

## More Information

The online help (Help > Online Help) and the Resources section (Help > Resources > Tips and Techniques) describe trusted scanning setup requirements and best practices. This information details the account requirements for each of the supported authentication types.



# Compliance Dashboard and Reports

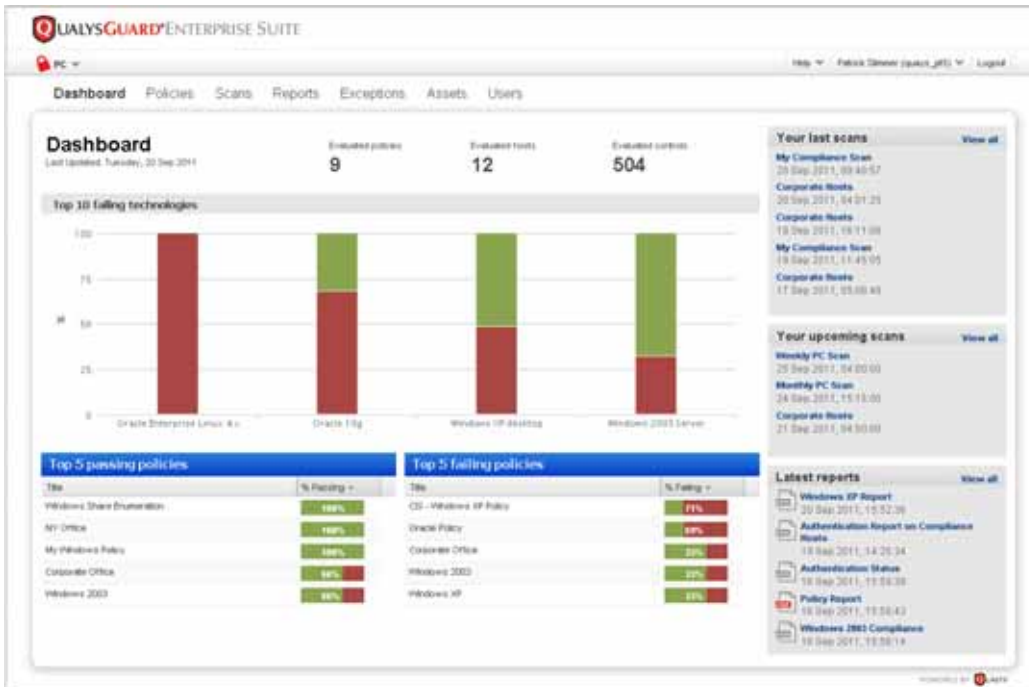
A policy compliance dashboard and specialized policy compliance reports provide compliance status information for the hosts in your account, based on the results returned from the most recent compliance scans. These reports help you identify whether hosts are compliant with the policies in your account.

Please note that the service updates compliance data in your account when the following actions take place: a policy is created or edited, an asset group that is assigned to a policy is edited, and a compliance scan (on demand or scheduled) is launched and completed successfully.

Authentication to target hosts is required for compliance scans. If authentication is not successful the service does not collect and update the compliance data in your account. See “Authentication to hosts” for more information.

## Dashboard

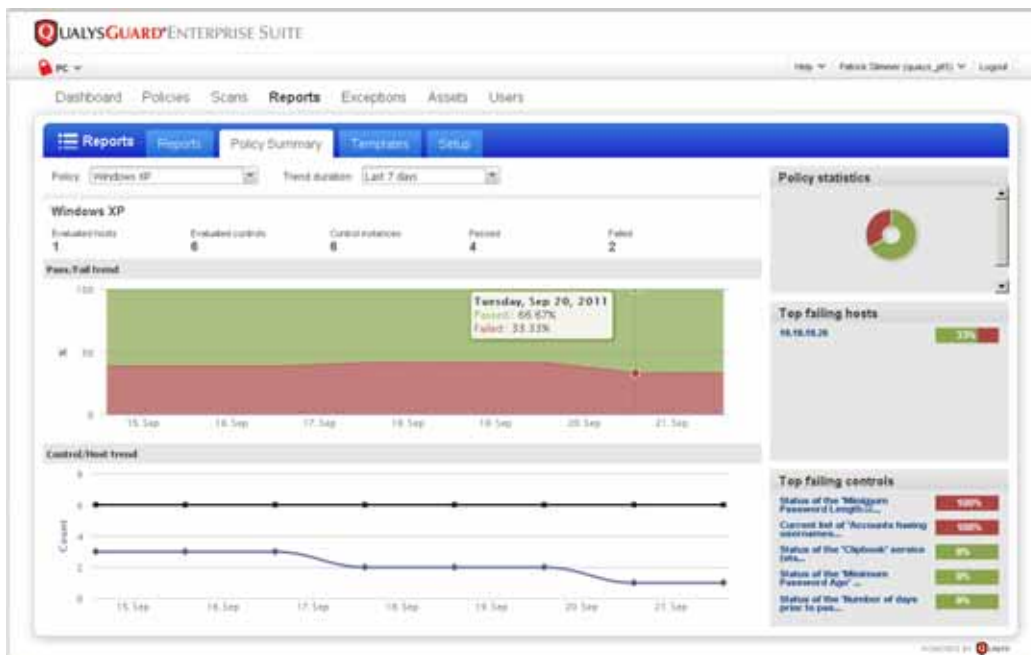
The policy compliance dashboard provides a summary of your overall compliance status across all policies in your account. It displays the top 10 failing technologies so you can prioritize your compliance efforts. From the dashboard, you can drill-down into a policy summary report for any policy listed, make changes to upcoming schedules, view compliance reports and more. To view the dashboard, select Dashboard on the top menu.



## Policy Summary

The Policy Summary provides a one-page summary of your compliance status for a specific policy in your account. You can view the Policy Summary from the Reports section (Reports > Policy Summary) or link to it from the PC Dashboard (double-click any policy title under Top 5 passing policies or Top 5 failing policies).

At the top of the page, select the policy you're interested in from the Policy menu. When you link to this page from the Dashboard the policy is selected for you. You can change the policy selection at any time to report on a different policy in your account. You can also change the trend duration selection from the Trend Duration menu. Your selection determines the number of days (7-90) included in the trend graphs. Note that trend graphs may show aggregate data when a longer time frame is selected.



You can run interactive compliance reports directly from the Policy Summary.

Select the IP address for any host listed under "Top failing hosts" to run the Individual Host Compliance Report for the selected host/policy.

Select the control title for any control listed under "Top failing controls" to run the Control Pass/Fail Report for the selected control/policy.

Interactive reports are described in more detail in the sections that follow.

## Compliance Reports

Policy compliance reports are available when Policy Compliance is enabled in your account. All Managers and Auditors can run these reports. Sub-account users (Unit Managers, Scanners, Readers) can run these reports when the compliance management option is enabled in their account. As with other reports, sub-account users can view the compliance data for their permitted IPs, in other words for the IPs in their own account.

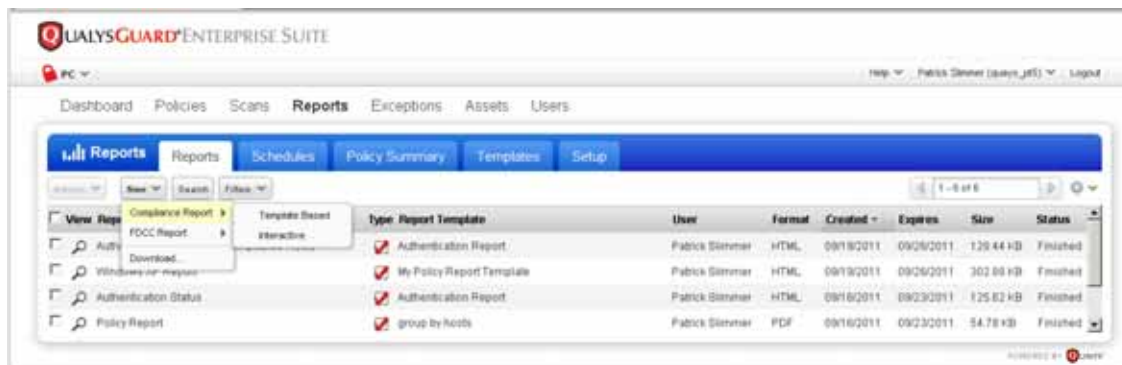
All policy compliance reports are based on the most recent compliance scan for each host. There are 2 template based reports and 2 interactive reports. Once generated, template based reports are saved to Report Share. Interactive reports are not saved to Report Share.

## Run compliance reports

To run a compliance report, select Reports from the top menu and click the Reports tab.

To run a template based report, go to New > Compliance Report > Template Based.

To run an interactive report, go to New > Compliance Report > Interactive.



## Authentication Report

The Authentication Report identifies whether authentication was successful for scanned hosts. If authentication to a host is not successful, then no controls can be evaluated for the host and no compliance data can be collected for the host. If authentication to a host is successful, then the host can be evaluated for compliance. The Authentication Report uses a hidden report template provided by the service. This template cannot be viewed from the report templates list.

To run the Authentication Report, select New > Compliance Report > Template Based. Select the report type Authentication Report. Select a report format, report source (certain business units or asset groups), and choose whether to display the Summary and/or Details section. Click Run.

## Schedule the Report (optional)

Click the Scheduling check box under Report Options to schedule the report to run automatically at a specified time. Set scheduling options to define when and how often this report should run. Click the Notification check box to set report notification options to have an email notification sent to select distribution groups when the report is finished and ready for viewing. Click Schedule.

**New Compliance Report** Launch Help

Use the following form to create a new report on compliance data.

---

**Report Details**

Title:

Report Type:

Report Format:

---

**Report Source\***

Select at least one business unit or asset group to draw data from.

Business Units

Asset Group:  [Select](#)

---

**Display & Filter**

Select the items you want to show in your report.

**Details**

Summary Section

Details Section

---

**Report Options**

**Scheduling**

Schedule this report to run automatically at the time you specify.

Start:       DST

Occurs:   days

**Notification**

Prohibit select distribution groups when the report is complete.

From:

Email To:  [Add Group](#)

Subject Line:

Custom Message:

The email will include general information about the report file, size and owner.

**Report Distribution Method** (Manager setting)

Attachment or Link. A report less than 1 MB will be sent as an attachment. If greater than 1 MB, a report link will be sent.

Password protect this report  
Recipients will be required to enter this password in order to download the report.

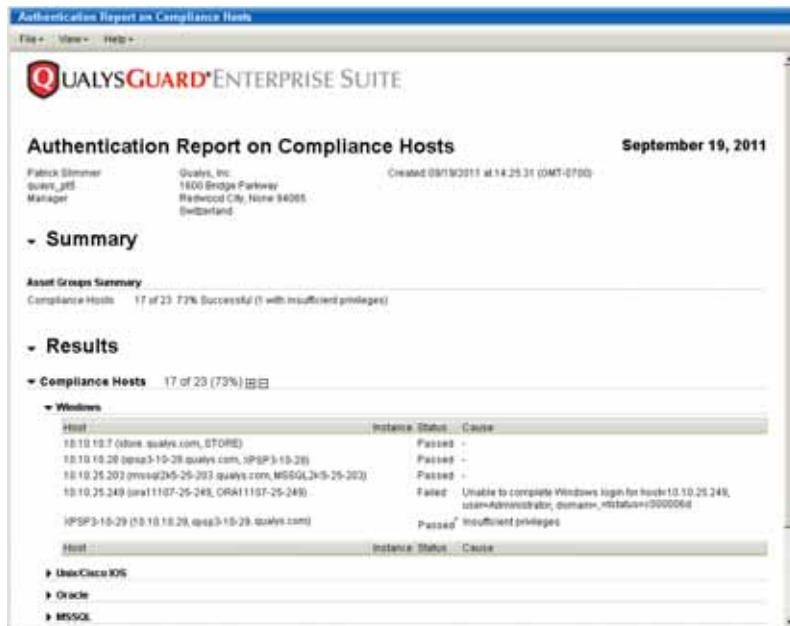
Restrict downloads  
Limit the number of times the report can be downloaded.

---

**Schedule Status**

Deactivate this report.

## Sample Authentication Report:



The Summary section of the report shows the total number of hosts that passed authentication for each asset group or business unit included in the report. For example, if your report shows “4 of 6 66%” then 6 hosts in the group were successfully scanned. Out of the 6 hosts scanned, authentication to 4 hosts was successful.

The Results section lists hosts you selected for the report source. If the service successfully authenticated to a host, then the status Passed appears. If the service did not authenticate to a host, then the status Failed appears along with the reason (cause) of the failure so that you can address it. If the service successfully authenticated to a host but the login account had insufficient privileges, then the status Passed\* appears. In this case, no posture evaluation could be performed on the host. Make sure the user account provided in the authentication record meets the minimum account requirements. Read “Authentication to hosts” for more information.

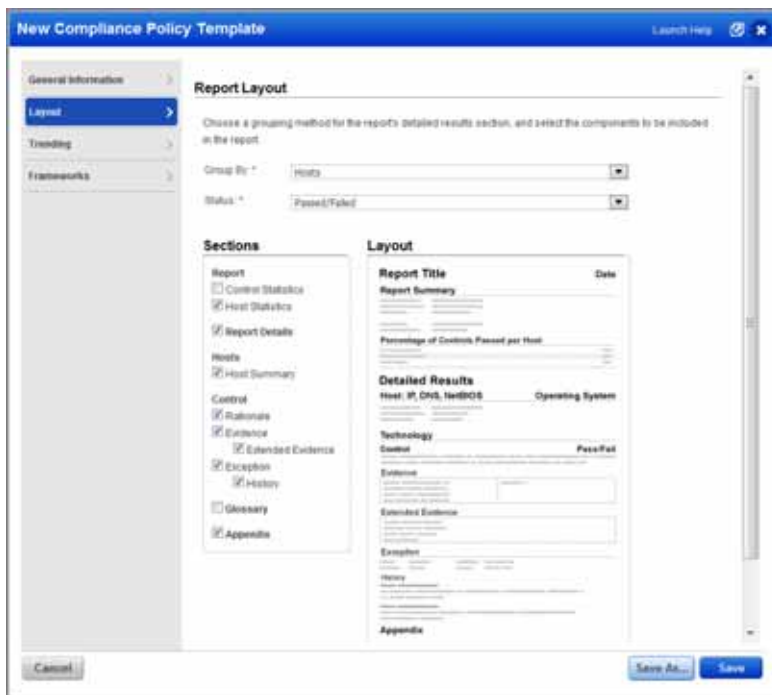
## Policy Report

The Policy Report identifies compliance status and trend information for a specific policy. The report lists hosts relevant to the policy with the controls tested on each host and the passed/failed status for each control. For each control, you can view the expected value as defined in the policy and the actual value returned when the host was last scanned.

### Create policy report template

The Policy Report requires a user-created policy report template. The template settings determine the layout and organization of your report, the trend duration for trend graphs, and the list of frameworks that may appear in the report.

You create policy report templates from the report templates list. Go to Reports > Templates. Then go to New > Policy Template. The New Compliance Policy Template wizard appears.



In the General Information section, provide a template title, change the owner and set global options. In the Layout section, determine the sorting method for report details (group by hosts or controls) and the sections that you want to include in the report. Each section selected in the template is included in the report. Clear a section to remove it from the report. As you clear options in the Sections area, those sections are removed from the Layout preview so that you can see how the report will look. In the Trending section, specify the trend duration period for the trend graphs included in the report. Select between 7-90 days (default is 30). In the Frameworks section, select the frameworks you want to include in the report: all available frameworks (as defined for the subscription) or a custom list of frameworks.

After making your template settings, click “Save” to save the report template. Your template appears in the report templates list. You can run this template at any time to generate a report.

## Run the Policy Report

To run the Policy Report, select New > Compliance Report > Template Based. In the New Compliance Report wizard, select the report type Policy Report and specify your policy report template in the Report Template field. Choose the policy you want to report on. Under Asset Groups you have the option to run the report on all asset groups in the policy or to select specific asset groups. Click Run.

## Schedule the Report (optional)

Click the Scheduling check box under Report Options to schedule the report to run automatically at a specified time. Set scheduling options to define when and how often this report should run. Click the Notification check box to set report notification options to have an email notification sent to select distribution groups when the report is finished and ready for viewing. Click Schedule.

**New Compliance Report** Launch Help

Use the following form to create a new report on compliance data.

**Report Details**

Title:

Report Type:

Report Template:  [Select](#)

Report Format:

**Report Source**

Select a policy to draw data from.

Policy:

Asset Groups

All Asset Groups in policy

Select asset groups

Policy Asset Groups:  [Select](#)

Note: Trend data will not appear in report unless all asset groups are included.

**Report Options**

**Scheduling**

Schedule this report to run automatically at the time you specify.

Start:     DST

Occurs:   days

**Notification**

Notify select distribution groups when the report is complete.

From:

Email To:  [Add Group](#)

Subject Line:

Custom Message:

The report will include general information like the report title, time and source.

**Report Distribution Method** (Manager setting)


Attachment or Link: A report less than 1 MB will be sent as an attachment. If greater than 1 MB, a report link will be sent.

Password protect this report  
Recipients will be required to enter this password in order to download the report.

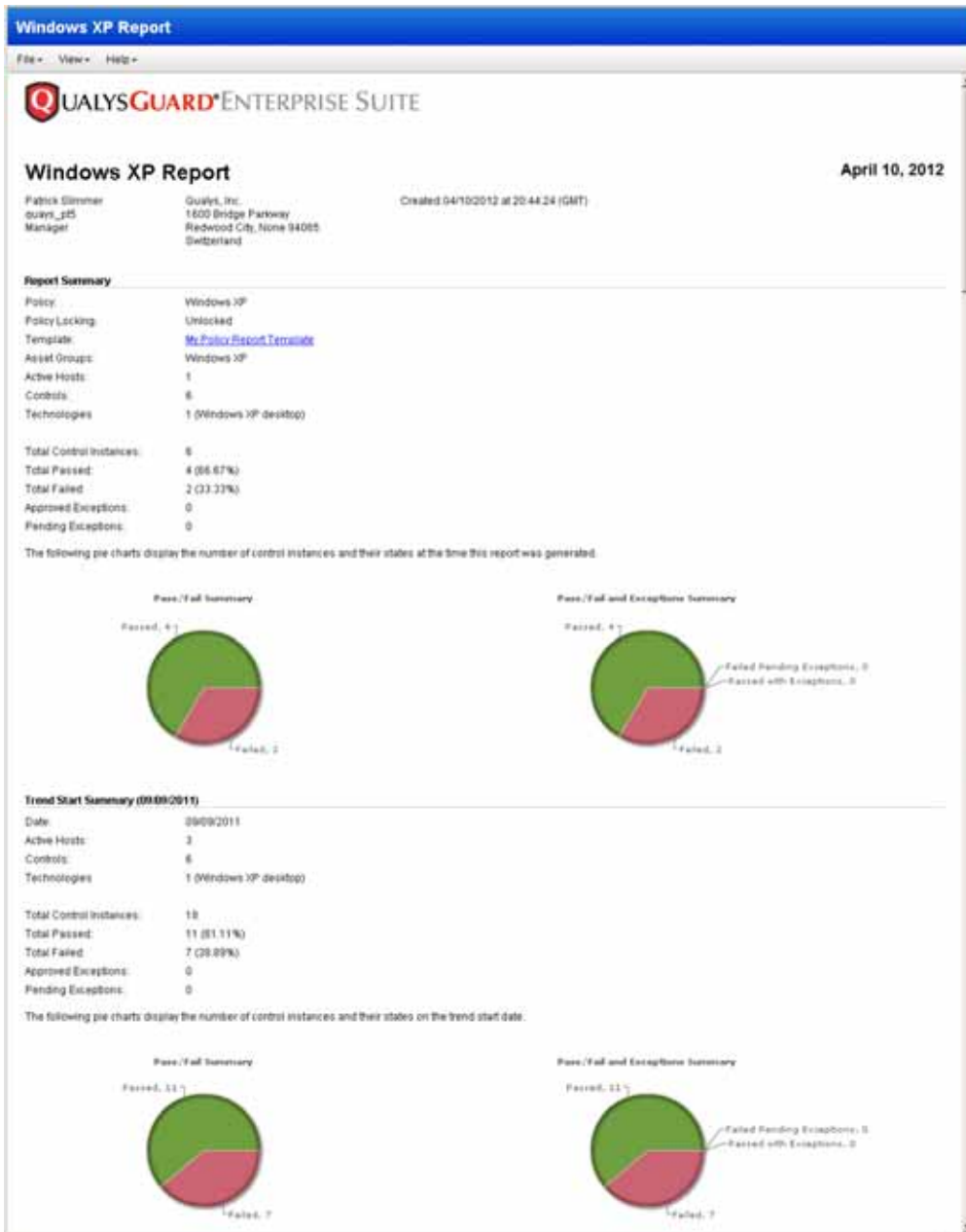
Restrict downloads  
Limit the number of times the report can be downloaded.

**Schedule Status**

Deactivate this report

The report runs in Report Share. If you close the New Report wizard, the report runs in the background. The completed report is available from the reports list, like other template based reports. To view the report, click  next to the report title.

Sample Policy Report:



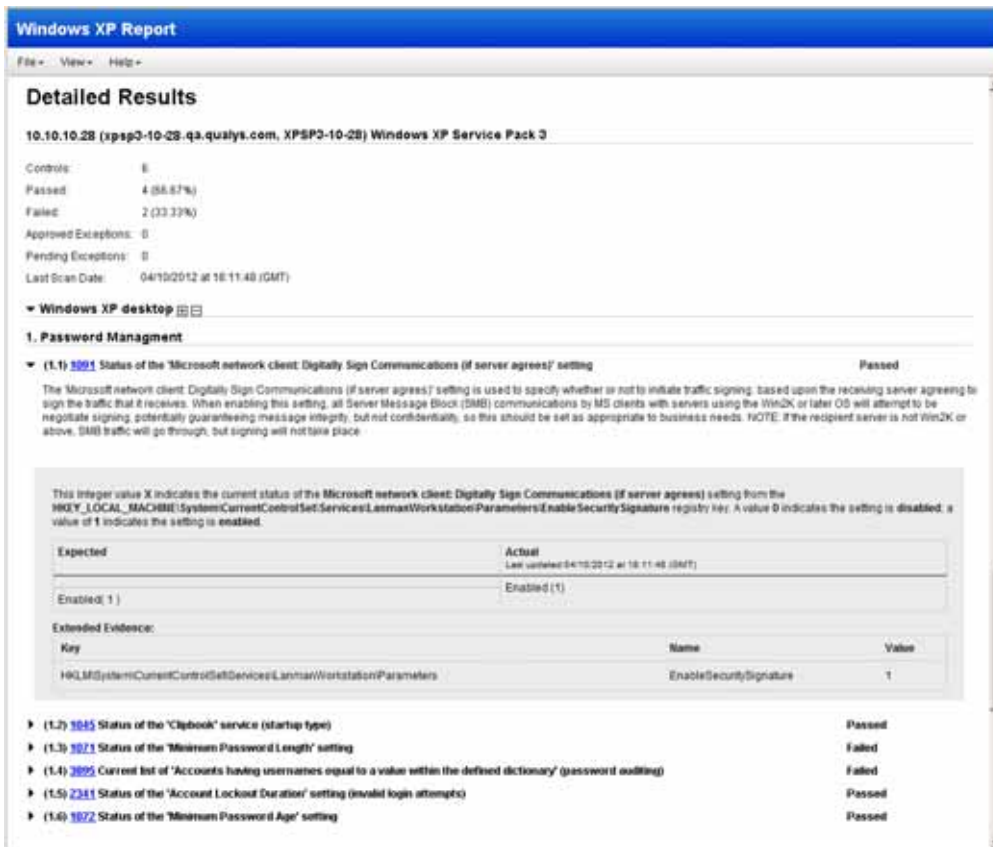
The Report Summary section of the report provides information known on the report generation date like the number of active hosts and controls in the policy, and the total number of control instances with a Passed or Failed status. The Trend Start Summary section of the report provides information known on the trend start date, which is determined by the trend duration set in the report template. For example, if the trend duration is set to 11 days, then the trend start date is 11 days prior to the report generation date.

Following the Trend Start Summary section are trend graphs. The Control Compliance over Time graph shows the total number of control instances at each status level over the trend duration period. The Active Hosts over Time graph shows the total number of active hosts for the policy over the trend duration period. A host is considered active when at least one control in the policy was evaluated on the host, resulting in a passed or failed status. The Controls over Time graph shows the total number of controls in the policy over the trend duration period. Users can add controls to a policy and remove controls from a policy at any time. Note that the graph shows the number of controls in the policy, not the number of control instances.

In the sample graphs below, the trend start date is September 8th and the report generation date is September 19th. The trend duration is set to 11 days.



Now scroll down further to see the Detailed Results section of the report.



The grouping method in the Detailed Results section depends on your policy report template settings. In the sample above, the results are grouped by hosts. For each host, a list of controls evaluated on the host appears with the resulting Passed or Failed status.

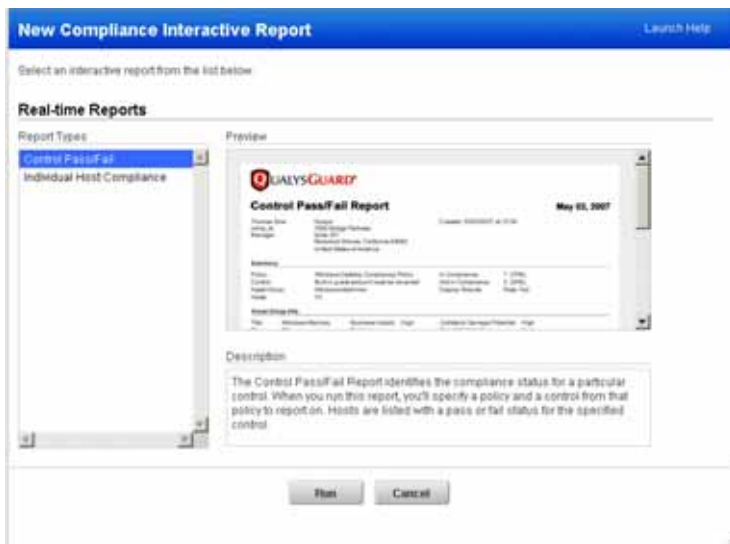
Click on any control statement to expand the control details to view the expected value and the actual value for the control on the host. The expected value is the value defined in the compliance policy. The actual value is the value returned during the last compliance scan on the host.

Make changes to the policy report template settings to change the grouping method or remove sections from the report.

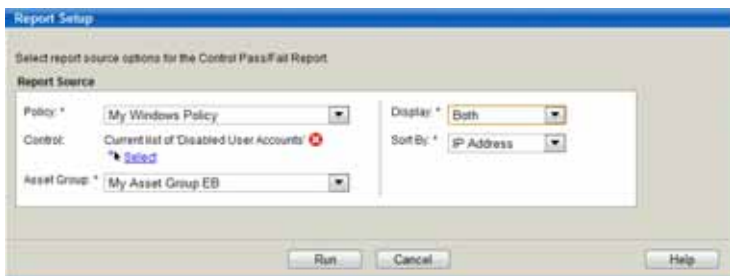
## Control Pass/Fail Report

The Control Pass/Fail Report identifies the pass/fail status for a specific control. When running this report, identify the policy and control you want to report on. Hosts included in the report are listed with a pass or fail status for the specified control.

To run the Control Pass/Fail Report, click the Reports tab and select New > Compliance Report > Interactive and then select Control Pass/Fail and click Run.



The report setup wizard prompts you to select report settings.



- 1 Select a policy in your account and a control within that policy.
- 2 Select an asset group that is assigned to the policy (this option is available to Managers and Auditors) to report on.
- 3 For Display, select whether you want to show hosts that passed the control, that failed the control, or both.
- 4 For Sort by, specify how you want the hosts to be sorted. Your options are: IP Address, NetBIOS name, DNS name, Posture, Exception (status).
- 5 Click Run to start report generation.

The completed report appears in the same window. Note that this report is dynamically generated and it is not saved in Report Share.

The Summary section provides a report summary. The Asset Group section that follows shows information about the target asset groups (this is visible only to Managers and Auditors). In the Results section, the hosts from the target asset group that the control applies to are listed.

Sample Control Pass/Fail Report:

**Report Results**

File View Help

Actions: Request Exception

**QUALYS GUARD ENTERPRISE SUITE**

**Control Pass/Fail Report**  
April 10, 2012

Jason Kim  
quyrs\_ah12  
Manager  
Qualys, Inc.  
1600 Bridge Parkway  
Redwood City, California 94065  
United States of America  
Created  
04/10/2012 at 21:31:16 (GMT)

**Summary**

Policy:	My Windows Policy	Hosts:	1
OID:	2443	In Compliance:	1 (100%)
Control:	Current list of Disabled User Accounts	Not in Compliance:	0
Asset Group:	My Asset Group EB	Display Results:	Both
		Sort By:	IP Address

**Asset Group Information**

Title:	My Asset Group EB	Business Impact:	High	Collateral Damage Potential:	Not Defined
IPs:	1	Division:	-	Target Distribution:	Not Defined
Domains:	0	Function:	-	Confidentiality Requirement:	Not Defined
Users:	1	Location:	-	Integrity Requirement:	Not Defined
				Availability Requirement:	Not Defined

**Results**

1.7 Current list of 'Disabled User Accounts'

IP Address	Tracking	DNIS	Hostname	NetBIOS	Hostname	Instance	OS	OS CPE	Posture	Exception
10.10.10.29	IP		spc3-10-29-28.g480h.adm.wm.ga.qualys.com				Windows XP Service Pack 3	spc3-10-29	Windows spc3 to mvcosoft/windows_xp_sp3	Passed

and/or drivefile shares. As this check can provide an inventory of all disabled User Accounts on any given system, which can then be compared to Human Resources' Terminated list, to ensure adherence to the company's security policies, this list should be audited and applied as appropriate to the needs of the business.

The following List String value(s) X provides an inventory of the disabled users on the system.

Expected	Actual
matches regular expression list	Guest HelpAssistant SUPPORT_388945a0

1 of 1 Items Shown, 0 selected

The Posture column identifies the status for the control on each host. Passed indicates that the expected value defined in the policy for the control matches the actual value returned during the last compliance scan on the host. Failed indicates that the expected value defined in the policy for the control does not match the actual value returned during the last compliance scan on the host. Passed<sup>E</sup> indicates that the host is exempt from the control. This means that an exception was requested and accepted for the control on the host. See “Managing exceptions.”

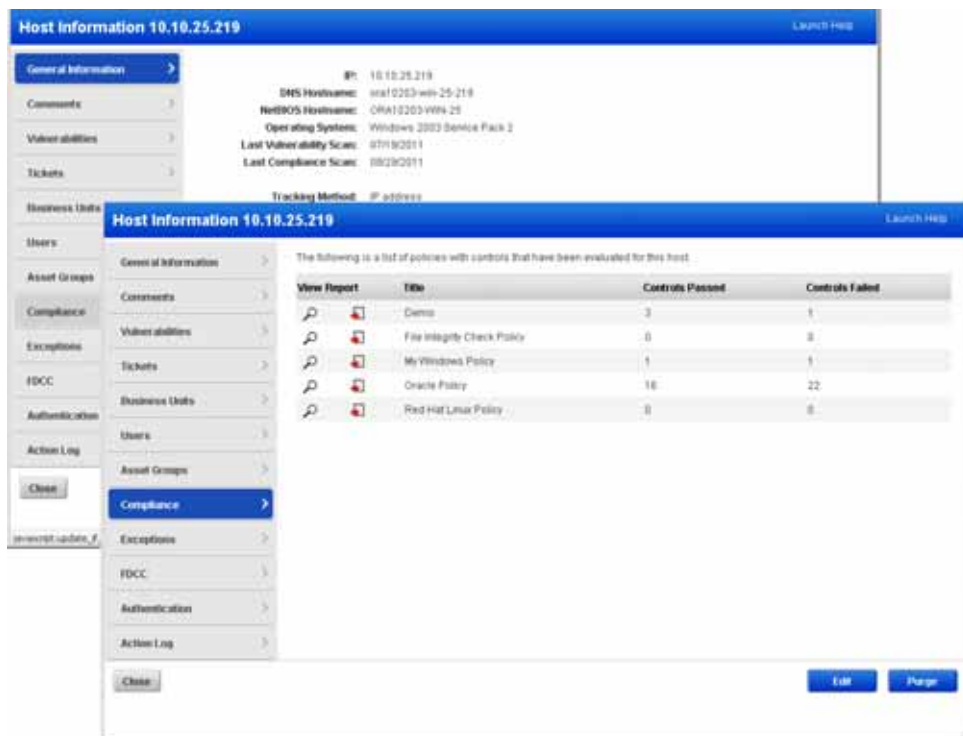
Additional report options:

**Setup Pane** — The report can be updated dynamically within the same window. Select **View > Setup Pane** to return to the Report Setup window, modify settings and run again.

**Preview Pane** — The preview pane is the area below your report results. When the report first appears the preview pane is shown, so you can select a host in the results section to see more information about it. Select **View > Preview Pane** to hide the preview pane to maximize the space for showing the results.

**Request Exception** — There may be times when users need to exempt hosts from certain controls in the policy. Users can submit exception requests from the Results section of the report. To do this, select the check box next to one or more hosts in the Results section that you wish to include in the request and then click the Request Exception button (at the top of the report). See “Managing exceptions.”

**View Host Information** — In the Results section, click an IP address to view host information about a particular IP in the Host Information view. The sample Compliance section (below) shows the current compliance data for the host:



The Compliance section includes a list of policies with controls that have been evaluated for the host. For each policy, the number of controls that passed and failed for the host are listed. For more information, follow the links provided. Click to view the policy settings. Click to run the Individual Host Compliance Report.

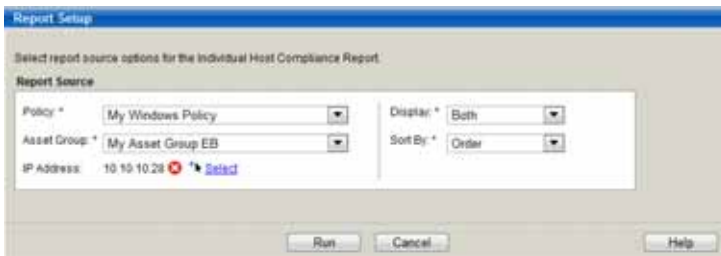
## Individual Host Compliance Report

The Individual Host Compliance Report identifies the compliance status for a specific host. When running this report, identify the policy and host you want to report on. Each control from the policy that is applicable to the host is listed with a pass or fail status.

To run the Individual Host Compliance Report, click the Reports tab and select New > Compliance Report > Interactive and then select Individual Host Compliance.



The report setup wizard prompts you to select report settings.



- 1 Select a policy in your account.
- 2 Select an asset group that is assigned to the policy (this option is available to Managers and Auditors).
- 3 Click the Select link to select a host (IP address) to report on.
- 4 For Display, select whether you want to show controls that passed for the host, that failed for the host, or both.
- 5 For Sort by, specify how you want hosts to be sorted. You may select one of these options: Order (the order of the controls in the policy), Control, Category, Posture, Exception (status).
- 6 Click Run to start the report generation.

The completed report appears in the same window.

The Summary section identifies the number of controls that passed and failed compliance for the host. The Results section lists host information: IP address, NetBIOS name (if appropriate), DNS name, the operating system detected on the host, the asset owner, and user-defined host attributes. The list area shows information for controls that are applicable to the host.

For each control, this policy information is shown: the policy section number, the control statement, the control category, the pass/fail status on the host, the exception status (appears only when the host posture on the control is Failed).

Sample Individual Host Compliance Report:

The screenshot shows the QualysGuard Enterprise Suite interface. The main title is "Individual Host Compliance" for "April 10, 2012". The asset is identified as "Jason Kim" (jaskim\_0112), Manager at Qualys, Inc. The report summary shows 22 controls, with 18 (72.73%) in compliance and 8 (27.27%) not in compliance. The results table lists four controls:

Order	CID	Control	Category	Posture	Exception
1.1	1071	Status of the Minimum Password Length setting	Access Control Requirements	Failed	<a href="#">Request</a>
1.2	1379	Status of the Microsoft network client Digitally Sign Communications (if server agrees) setting		Passed	
1.3	1111	Current content of the logon banner (Windows/Linux) / Permissions set for the /etc/issue file (Linux/Linux)	Access Control Requirements	Failed	<a href="#">Request</a>
1.4	3693	Current list of Accounts having empty password fields (password auditing)	Access Control Requirements	Failed	<a href="#">Request</a>

Additional report options:

Setup Pane — The report can be updated dynamically within the same window. Select View > Setup Pane to return to the Report Setup wizard, modify settings and run again.

Preview Pane — The preview pane is the area below your report results. When the report first appears the preview pane is shown, so you can select a control in the results list to see more information about it. Select View > Preview Pane to hide the preview pane to maximize the space for showing the results.

Request Exception — There may be times when users need to exempt hosts from certain controls in the policy. Users can submit exception requests from the Results section of the report. To do this, select the check box next to one or more controls in the Results section that you wish to include in the request, and then click the Request Exception button. See “Managing exceptions.”

View Control Scan Results — In the Results section, click on a control in the list to display scan results for the control on the host. The Expected value is the value as defined in the policy. The Actual value represents the compliance data retrieved from the most recent compliance scan. The service compares the actual value to the expected value to determine the compliance status.

The sample control results pane in the Report Results window (below) shows the scan results for the technical control (CID) 3895 titled “Current list of ‘accounts having usernames equal to a value within the defined dictionary’ (password auditing).”

**Report Results**

File View Help

Actions: Request Exception

**Results**

10.10.10.28 Windows XP Service Pack 3

IP Address: 10.10.10.28 Owner: --  
 CID Name: spsp3-10-28\_patch\_ad\_suh\_qa\_qualys.com Location:  
 Network Name: JPPSP3-10-28 Function:  
 OS: Windows XP Service Pack 3 Asset Tag:  
 OS CPE: cpe:/o:microsoft/windows\_xp:sp3:

Order	CID	Control	Category	Feature	Exception
1.1	1071	Status of the 'Minimum Password Length' setting	Access Control Requirements	Failed	<a href="#">Request</a>
1.2	1379	Status of the 'Microsoft network client 'Digitally Sign Communications if server agrees' setting		Passed	
1.3	1111	Current content of the logon banner (Windows/Unix/Linux) / Permissions set for the 'etc/passwd' file (Unix/Linux)	Access Control Requirements	Failed	<a href="#">Request</a>
1.4	3893	Current list of 'Accounts having empty password fields' (password auditing)	Access Control Requirements	Failed	<a href="#">Request</a>
1.5	3895	Current list of 'Accounts having usernames equal to a value within the defined dictionary' (password auditing)	Access Control Requirements	Failed	<a href="#">Request</a>
1.6	3894	Current list of 'Accounts having usernames matching their containing passwords' (password auditing)	Access Control Requirements	Failed	<a href="#">Request</a>
1.7	2441	Current list of 'Disabled User Accounts'	Access Control Requirements	Passed	
1.8	1864	Current list of 'Installed patches from the manufacturer (Microsoft)'	OS Security Settings	Passed	

**1.5 - Current list of 'Accounts having usernames equal to a value within the defined dictionary' (password auditing) [10.10.10.28]**

Username and password combinations are the fundamental building blocks to computer security. Without the use of them, there could be no valid expectation of confidentiality, integrity and availability of systems and/or data residing on them. As the 'frontline' of security, these username/password combinations should be setup in a way that they cannot easily be guessed by a malicious user whose intentions are to illegally or inappropriately access sensitive/confidential information for personal gain or to cause damage. Running this check periodically can help to ensure all username/password combinations are configured according to internal standards. A list of all accounts having usernames that appear in the 'Dictionary' provided will be the output of this check.

The following LAM string value(s) X indicate the current list of usernames that match passwords provided in the 'Dictionary'. The reported values will be base64 encoded.

Expected	Actual
is contained in regular expression list No accounts found No defined dictionary found.	LAM updated 04/10/2012 at 10:11:40 (GMT)

22 of 22 Items Shown, 0 selected

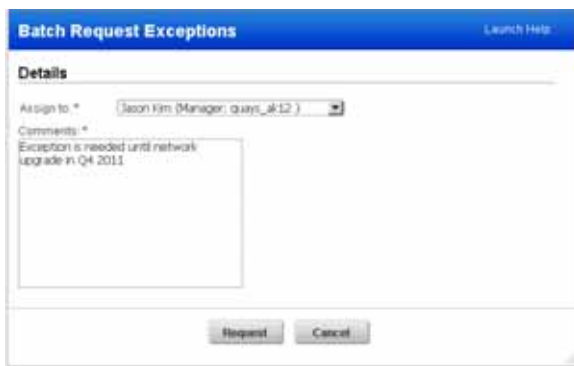
## Managing exceptions

Users may request exceptions for some hosts/controls in a selected policy to support a business need. For example a compliance policy may have a control that states the service FTP is not allowed on a server, however there may be a business requirement to exempt one or more hosts from this particular control in the policy. Users submit exceptions for one or more hosts/controls in a policy that failed compliance. When approved, compliance reports do not fail compliance for the hosts/controls in the exception request for a period of time defined in the request.

The exceptions workflow allows all users to submit and view exception requests and their status. Managers and Auditors can approve exception requests; Unit Managers may approve requests submitted by users in their business unit when this privileges is granted in their user account. User actions on exceptions are logged in the exception history.

## Submit exception requests

Users submit exception requests for any control in a policy that fails for a particular host. You submit exceptions from interactive compliance reports using the Request Exception workflow. When viewing a Control Pass/Fail Report, select host(s) in the results list. When viewing an Individual Host Compliance Report, select control(s) from the results list. After making selections click the Request Exception button. When prompted, assign to a user and add comments.



**Batch Request Exceptions** Launch Help

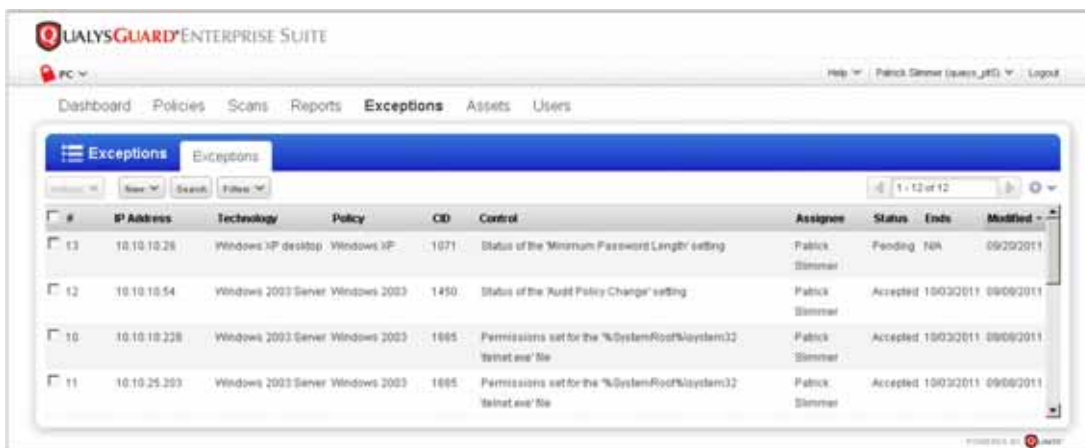
**Details**

Assign to \* Jason Kim (Manager: ouays\_jk12)

Comments \*  
Exception is needed until network upgrade in Q4 2011


## View exception requests

To view exception requests, select Exceptions on the top menu. The exceptions list appears. Each exception request has a status of: Pending (pending approval, when first submitted by a user), Accepted, Rejected, or Expired. When an exception request is accepted it is assigned a due date.




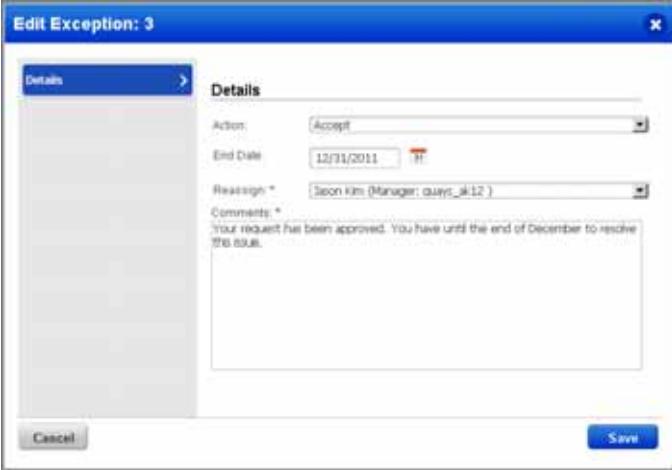
#	IP Address	Technology	Policy	CID	Control	Assignee	Status	Ends	Modified
13	10.10.10.26	Windows XP desktop	Windows XP	1071	Status of the Minimum Password Length setting	Patric Stimmer	Pending	NA	09/29/2011
12	10.10.10.54	Windows 2003 Server	Windows 2003	1450	Status of the Audit Policy Change setting	Patric Stimmer	Accepted	19/03/2011	09/08/2011
10	10.10.10.228	Windows 2003 Server	Windows 2003	1065	Permissions set for the '%SystemRoot%\system32\bin\cmd.exe' file	Patric Stimmer	Accepted	19/03/2011	09/08/2011
11	10.10.25.203	Windows 2003 Server	Windows 2003	1065	Permissions set for the '%SystemRoot%\system32\bin\cmd.exe' file	Patric Stimmer	Accepted	19/03/2011	09/08/2011

Use the Filter menu above the list area to filter the list to only show your assigned exception requests or the requests that you submitted. Use the Search option to find requests based on their attributes (status, assignee, host, control, and more).

To view detailed information about an exception, mouse over an exception row, click , and then select Info from the Quick Actions menu. The General Information section displays information about the policy and the host that failed compliance. Go to the History section to see actions taken on the exception.

## Accept/Reject exception requests

Managers and Auditors have privileges to accept and reject exception requests. Unit Managers may be granted this privilege for users in their business unit. To do this, go to the exceptions list and edit an exception. Mouse over an exception row and click  then select Edit from the Quick Actions menu. In the Edit Exception wizard, select Accept from the Action drop-down menu and assign an expiration (end) date.



The screenshot shows a web-based dialog box titled "Edit Exception: 3". It has a "Details" tab selected. The "Action" dropdown menu is set to "Accept". The "End Date" is set to "12/31/2011". The "Reassign" dropdown menu is set to "Seon Kim (Manager: ouqst\_uk12)". The "Comments" field contains the text: "Your request has been approved. You have until the end of December to resolve the issue." There are "Cancel" and "Save" buttons at the bottom of the dialog.

## Exception Notification

Users can select the Exception Notification option in their account settings (under Notification Options) when policy compliance is enabled. By selecting "My exceptions" the service sends you notifications for exceptions that you created and exceptions that have been assigned to you. The service sends notifications when an exception is requested and there is a change in its status.

# Contact Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at [www.qualys.com/support/](http://www.qualys.com/support/).