



# QualysGuard<sup>®</sup> Malware Detection Service Enterprise Edition

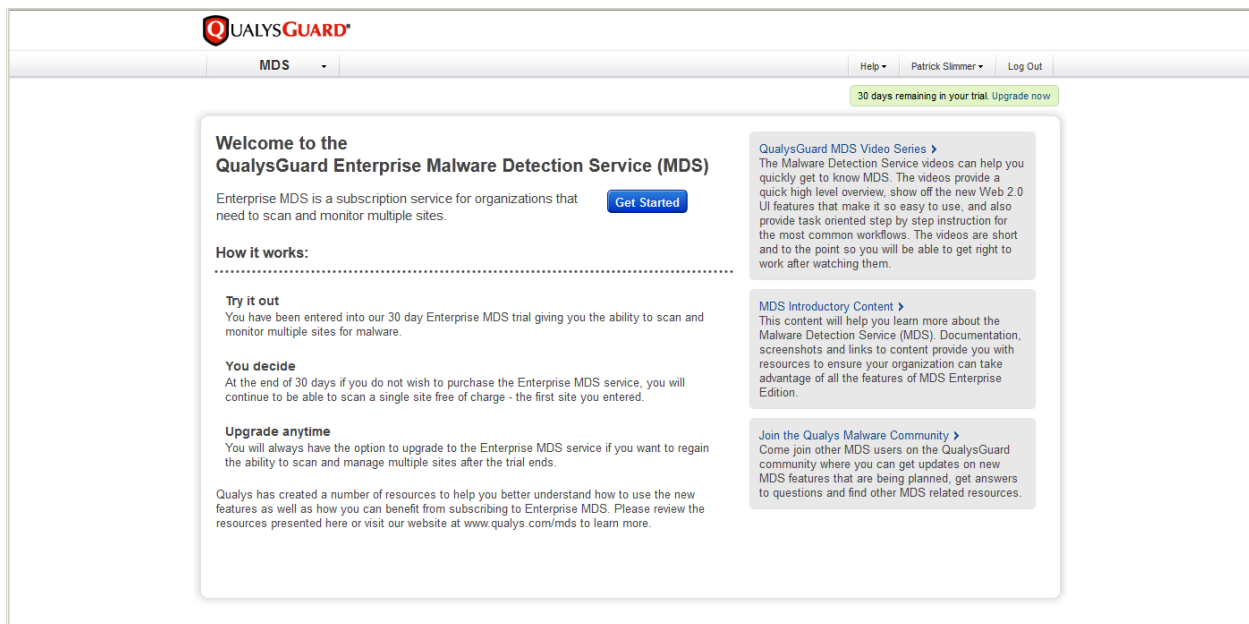
Getting Started Guide  
February 15, 2012

## Welcome

QualysGuard Malware Detection Service (MDS) Enterprise Edition is a new subscription service for organizations that need to scan and monitor a large number of sites for malware.

You're invited to take a 30 day trial of the QualysGuard MDS Enterprise Edition. At the end of the 30 days if you do not wish to purchase this new service, you will continue to be able to scan a single site free of charge (the first site that was added). You always have the option to upgrade to the QualysGuard MDS Enterprise Edition after the trial ends if you want to regain the ability to scan multiple sites.

After accepting Terms & Conditions, a Welcome page appears with links to a number of resources explaining the enhancements to MDS and the many benefits of the QualysGuard MDS Enterprise Edition.

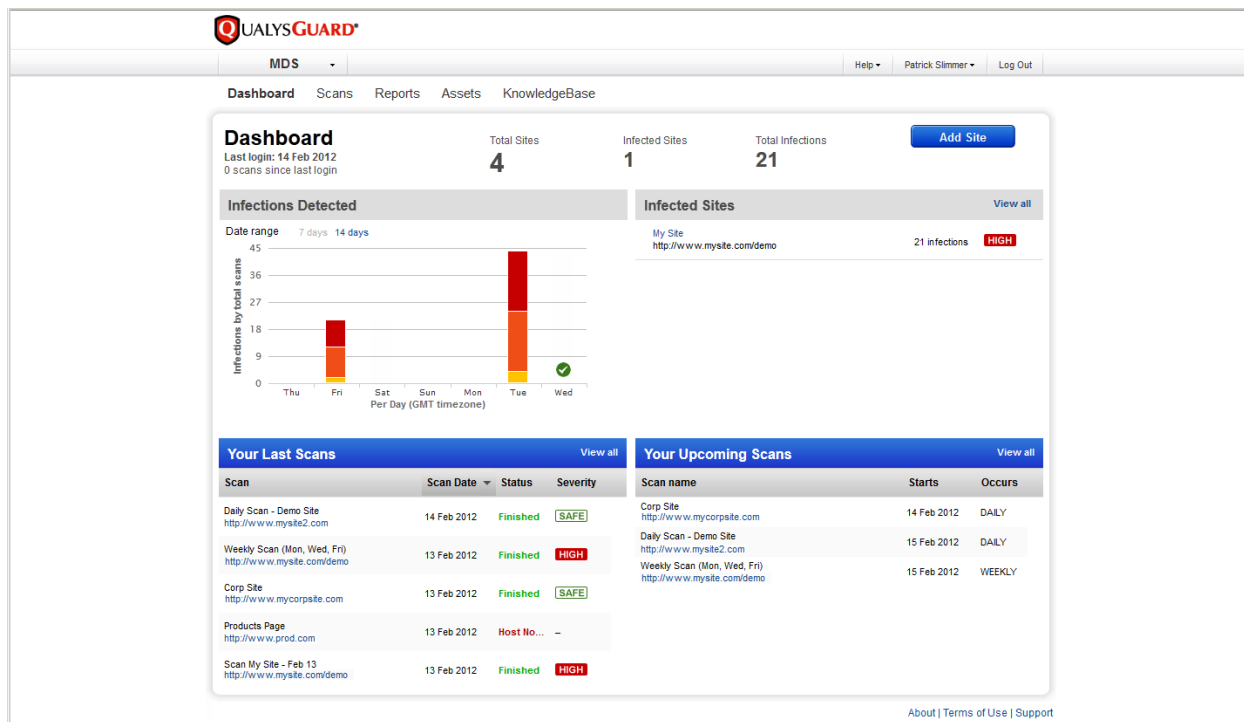


## Get Started

Click the Get Started button to start using the QualysGuard MDS Enterprise Edition service. Let's take a look now at the new user interface and how to get started.

## Dashboard

When you log into the service, the first screen to appear is your dashboard. The dashboard provides a comprehensive view of your scan activity based on the most recent scan results. If no scans have been launched in your subscription, then there will be no data to report.



Your dashboard includes these sections:

**Summary** – The top of the dashboard shows the total number of sites in your account, the number of sites with at least one infection, and the total number of infections across all sites.

**Infections Detected** – This graph displays the number of infections detected by all scans over the last 7 days or 14 days. Mouse-over any day to see the number of infections by severity level. Note that this graph includes the sum of all detections by all scans completed on each day. That means if you scan the same site more than once in the same day and the same infections are detected, then the infections will be counted more than once. A green check (✓) indicates that scans were completed but no detections were found. An empty bar indicates one of the following: 1) no scans were launched on that day, 2) scans were launched but they were cancelled or had an error before any detection was found, or 3) scans were launched but there was no host alive.

**Infected Sites** – This is a list of sites in your account with infected pages. Click the site title to view the pages on the site where malware was detected.

**Your Last Scans** – This is a list of the last 5 scans launched on sites in your account. The most recent scan is listed first. The scan status is shown for each scan as well as the highest severity level detected by the scan (for finished scans only). A severity level of SAFE indicates that the scan finished and no malware was detected by the scan.

**Your Upcoming Scans** – This is a list of the next 5 scans scheduled to run.

## Add a Site to Scan

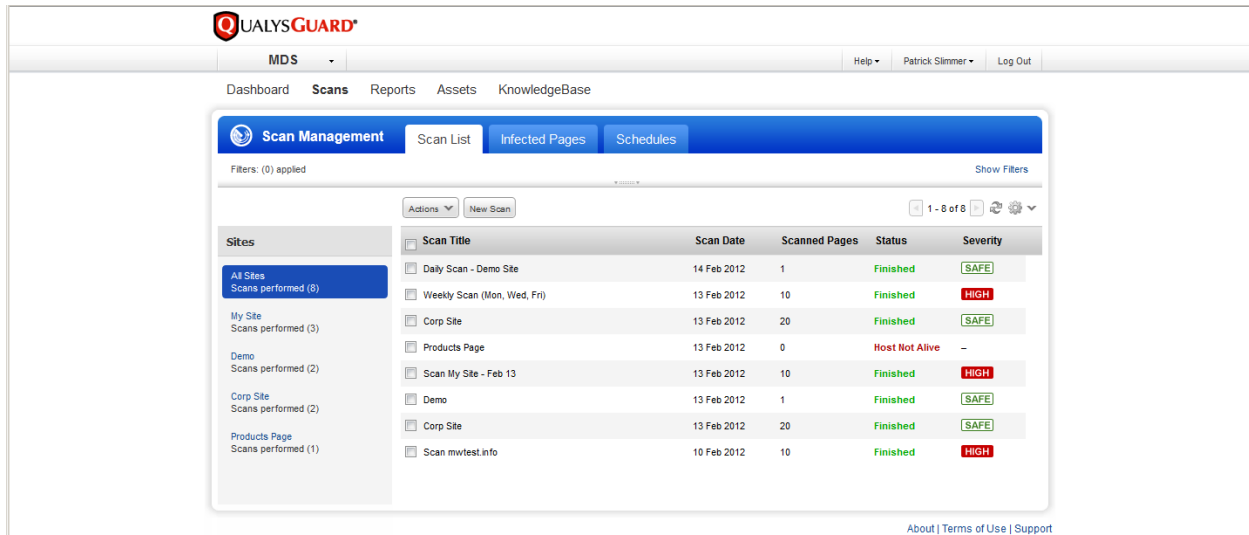
The first step to scanning for malware is to add the site you want to scan to your account. Click the Add Site button on your dashboard and then provide site details, scan options and set scheduling options to automatically scan the site on a recurring basis (optional). (Note: Turn on help tips in the wizard title bar to view online help for each of the settings. When turned on, help tips will display when you mouse over field names.)

A quick way to add several sites at once is to upload them from a CSV file. Simply select the “I have a CSV file to upload” check box (shown above) and then browse to your CSV file. Please make sure the CSV file is formatted correctly by following the guidelines that appear on the screen.

Newly added sites appear on the Sites list in the Asset Management section. To see this list and manage the sites in your account, select Assets on the top menu.

## Scans

Select Scans to go to Scan Management. The Scan List tab is where you view scan history, launch new scans, cancel scans in progress, and view the results of completed scans.

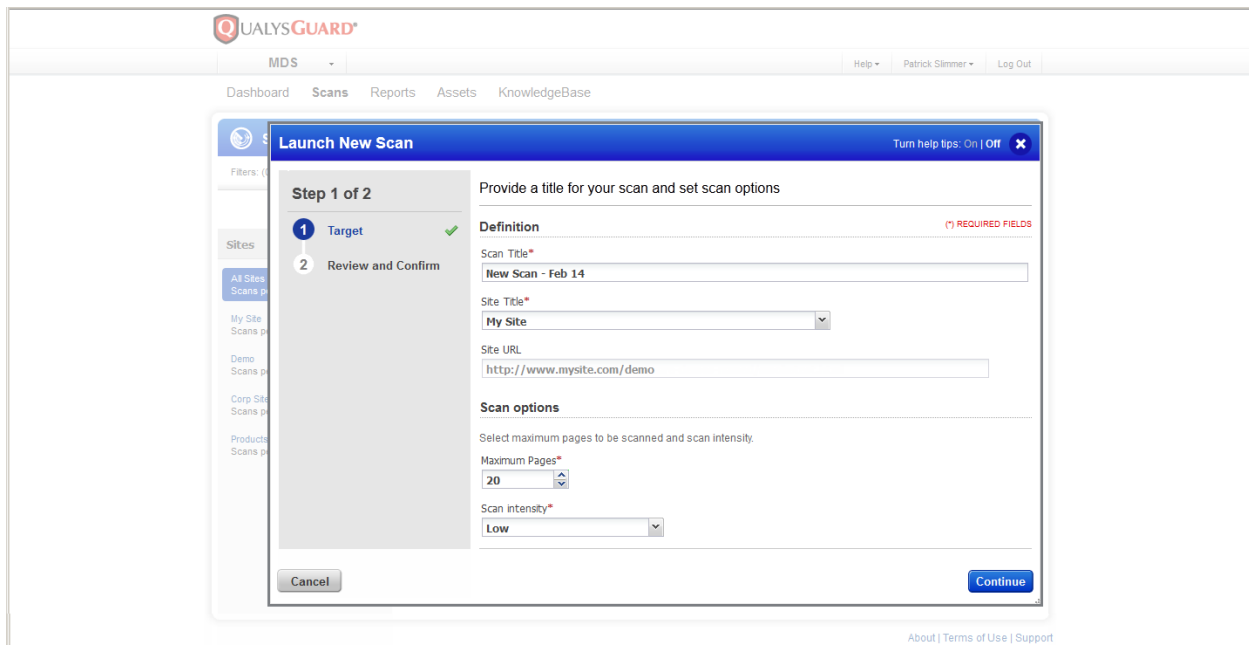


The screenshot shows the QualysGuard MDS interface. The top navigation bar includes 'MDS', 'Help', 'Patrick Slimmer', and 'Log Out'. The main navigation menu has 'Dashboard', 'Scans', 'Reports', 'Assets', and 'KnowledgeBase'. The 'Scan Management' section is active, with sub-tabs for 'Scan List', 'Infected Pages', and 'Schedules'. A sidebar on the left lists various sites and the number of scans performed for each. The main content area displays a table of scan results.

Scan Title	Scan Date	Scanned Pages	Status	Severity
Daily Scan - Demo Site	14 Feb 2012	1	Finished	SAFE
Weekly Scan (Mon, Wed, Fri)	13 Feb 2012	10	Finished	HIGH
Corp Site	13 Feb 2012	20	Finished	SAFE
Products Page	13 Feb 2012	0	Host Not Alive	-
Scan My Site - Feb 13	13 Feb 2012	10	Finished	HIGH
Demo	13 Feb 2012	1	Finished	SAFE
Corp Site	13 Feb 2012	20	Finished	SAFE
Scan mvtest.info	10 Feb 2012	10	Finished	HIGH

## Launch a New Scan

If you defined a scan schedule when creating your site, then your scan will run automatically at its scheduled time. You can also launch scans on demand. To do so, click the New Scan button. Then use the Launch New Scan wizard to define scan settings.

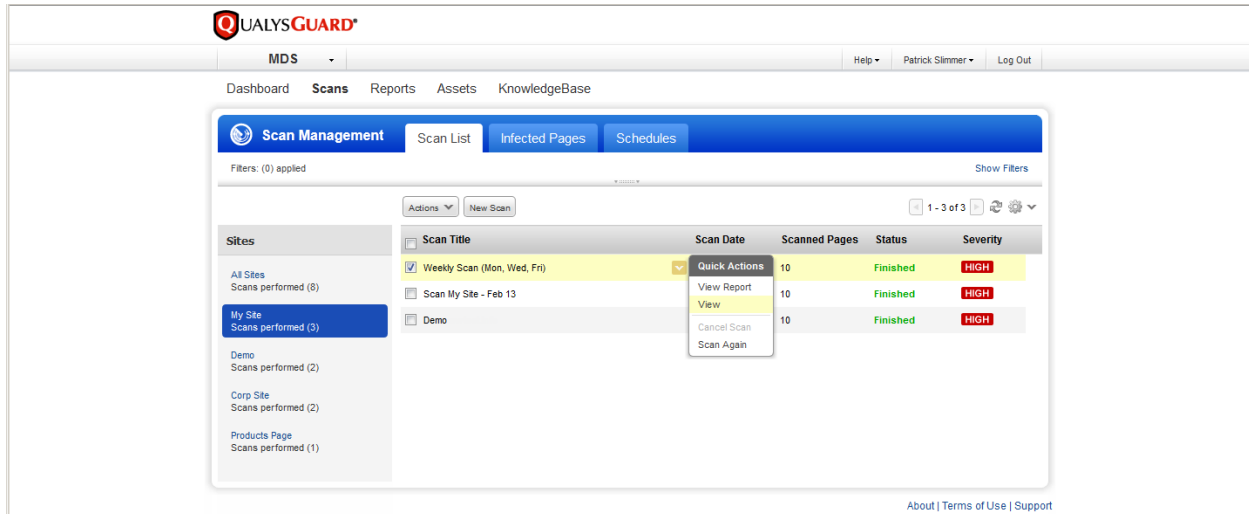


The screenshot shows the 'Launch New Scan' wizard in the QualysGuard MDS interface. The wizard is titled 'Launch New Scan' and has a progress indicator showing 'Step 1 of 2' with 'Target' selected and 'Review and Confirm' next. The 'Definition' section includes fields for 'Scan Title\*' (New Scan - Feb 14), 'Site Title\*' (My Site), and 'Site URL' (http://www.mysite.com/demo). The 'Scan options' section includes 'Maximum Pages\*' (20) and 'Scan intensity\*' (Low). There are 'Cancel' and 'Continue' buttons at the bottom.

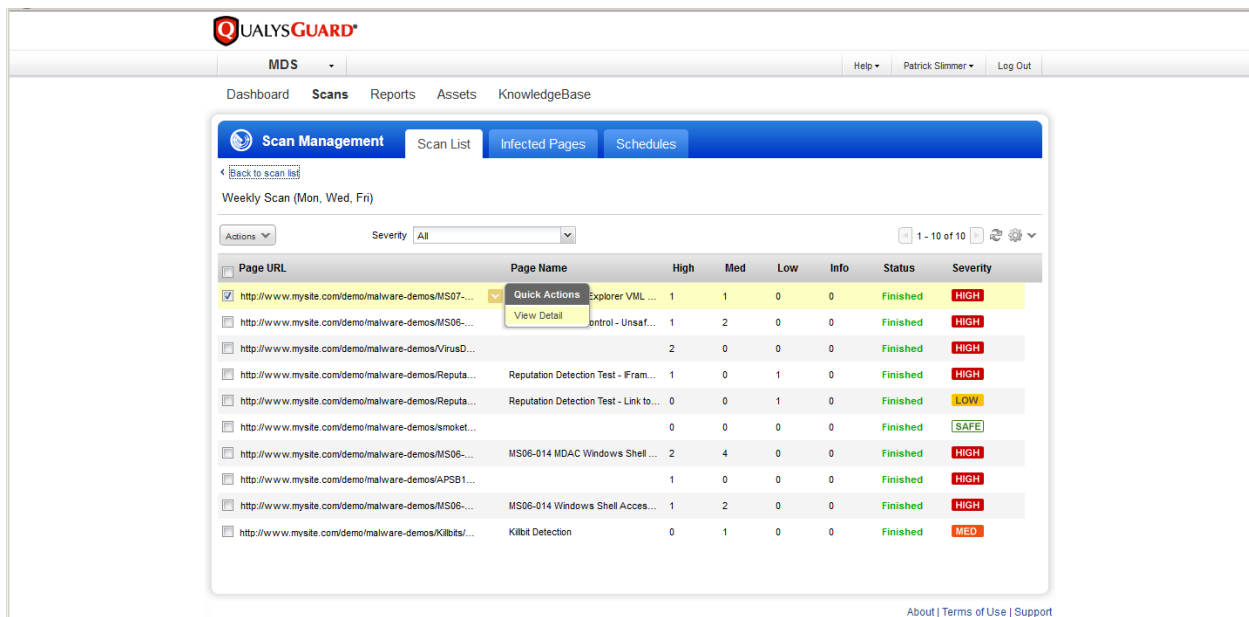
If malware infections are detected by the scan then you will be alerted by email. Log back into the service to view the complete scan results and generate reports.

## View Scan Results

When a scan is finished, you can view the scan results from the Scan List tab under Scans. Use filters to help you quickly identify the scan you're interested in. To only display scans launched on a particular site, select the site name from the Sites list on the left side of the screen. Additional filters are available by clicking the Show Filters link above the list area. Once you've identified the scan you're interested in, double-click the scan row (or select View from the Quick Actions menu).

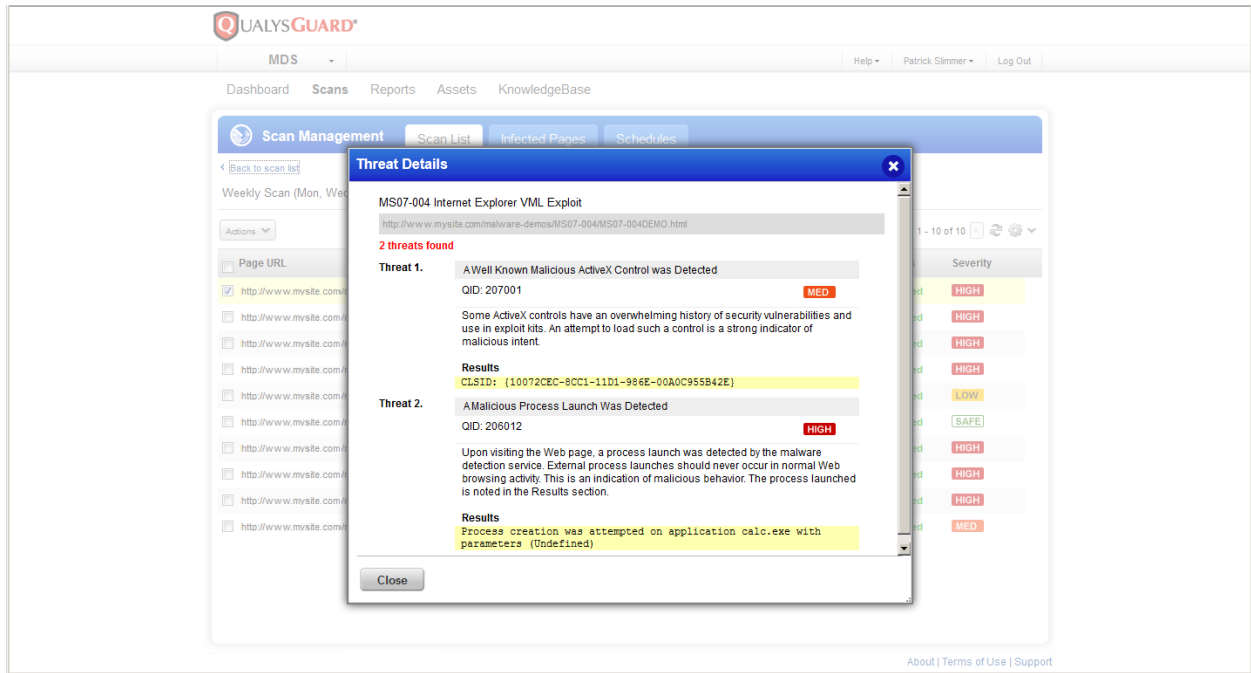


A list of pages on the site that were scanned appears. For each page, the following information is shown: the number of detections found at each severity level (High, Medium, Low, Info), the highest severity level detected for the page (in the Severity column) and the scan status.



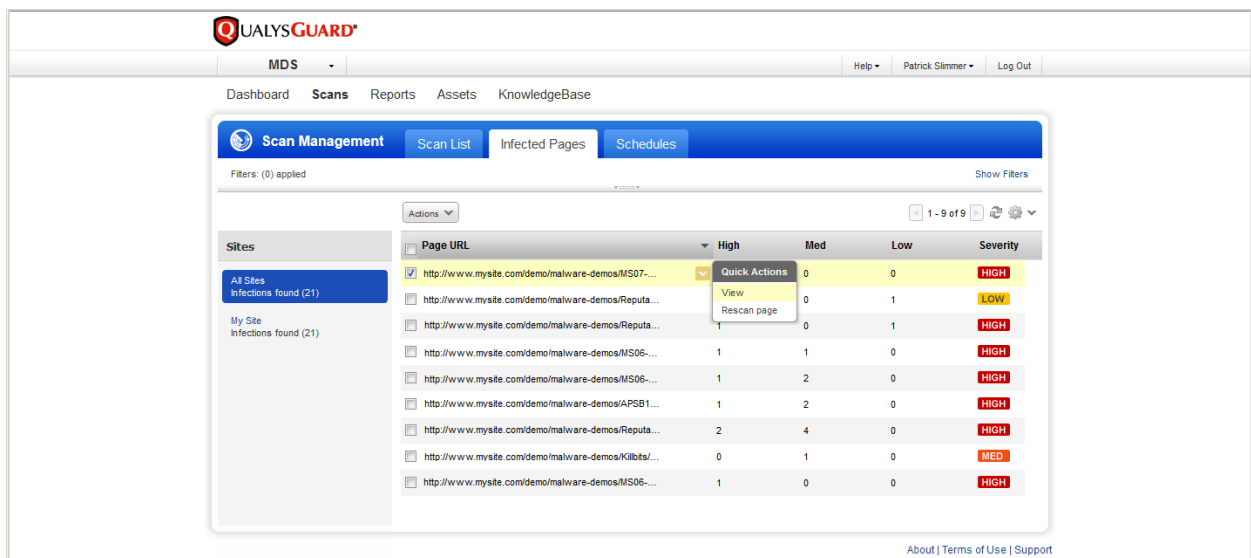
Now double-click a page row (or select View Detail from the Quick Actions menu) to see specific threats detected for the page.

The Threat Details window appears with the number of threats found on the page. For each threat, the following information is shown: the threat name, QID, severity, description and specific scan test results returned by the scan engine.



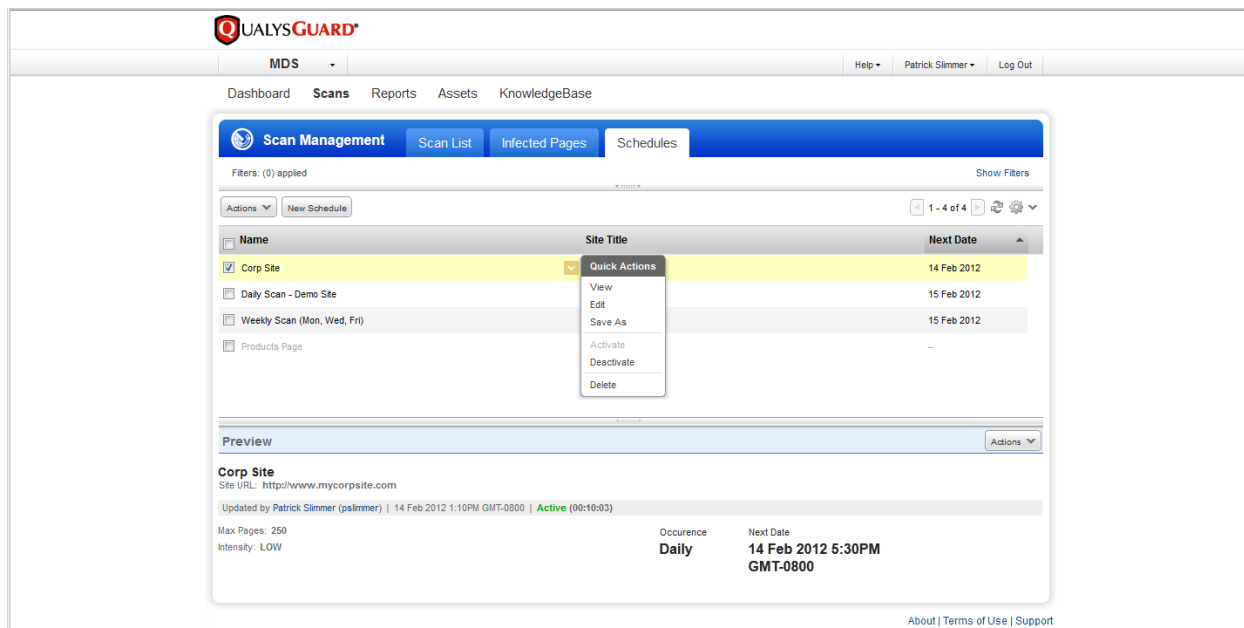
## View Infected Pages

To see all scanned pages where malware was detected, go to Scans and click the Infected Pages tab. From this list, you can drill-down into threat details for any page on any site and rescan a specific page.



## Manage Scan Schedules

The service supports regularly scheduled scanning to monitor sites on an ongoing basis with email alerts to quickly notify you when infections are detected. You can schedule scans to run daily, weekly or monthly. To manage scan schedules, go to Scans and click the Schedules tab. From this list you can create new schedules for the sites in your account, and take actions on existing schedules.



## Reports

Select Reports to go to Report Management. This is where you generate and save new reports, download reports, and securely distribute encrypted PDF reports to other users.

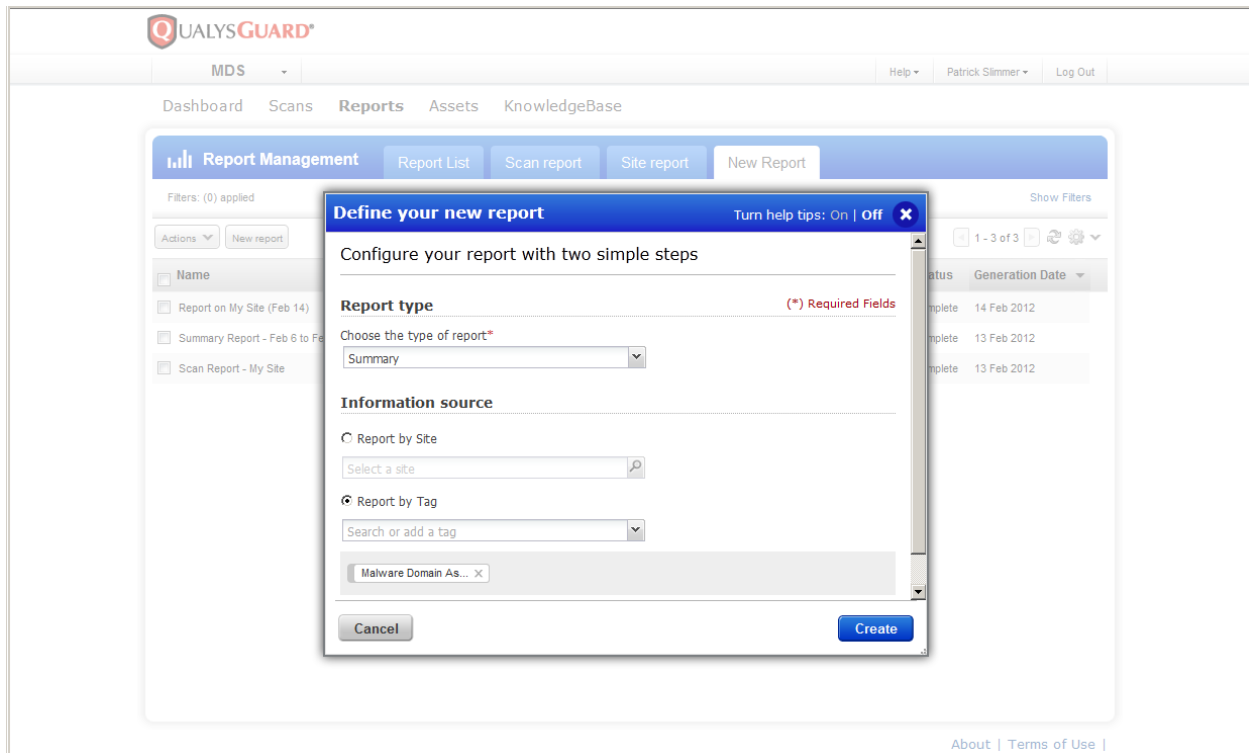
These report types are available:

- Scan Report – Report on results from a single scan.
- Site Report – Report on results for a single site or all sites with a specified tag.
- Summary Report – Generate an interactive report with a summary of the scans launched over a selected date range. This report may be run on a single site or all sites with a specified tag.

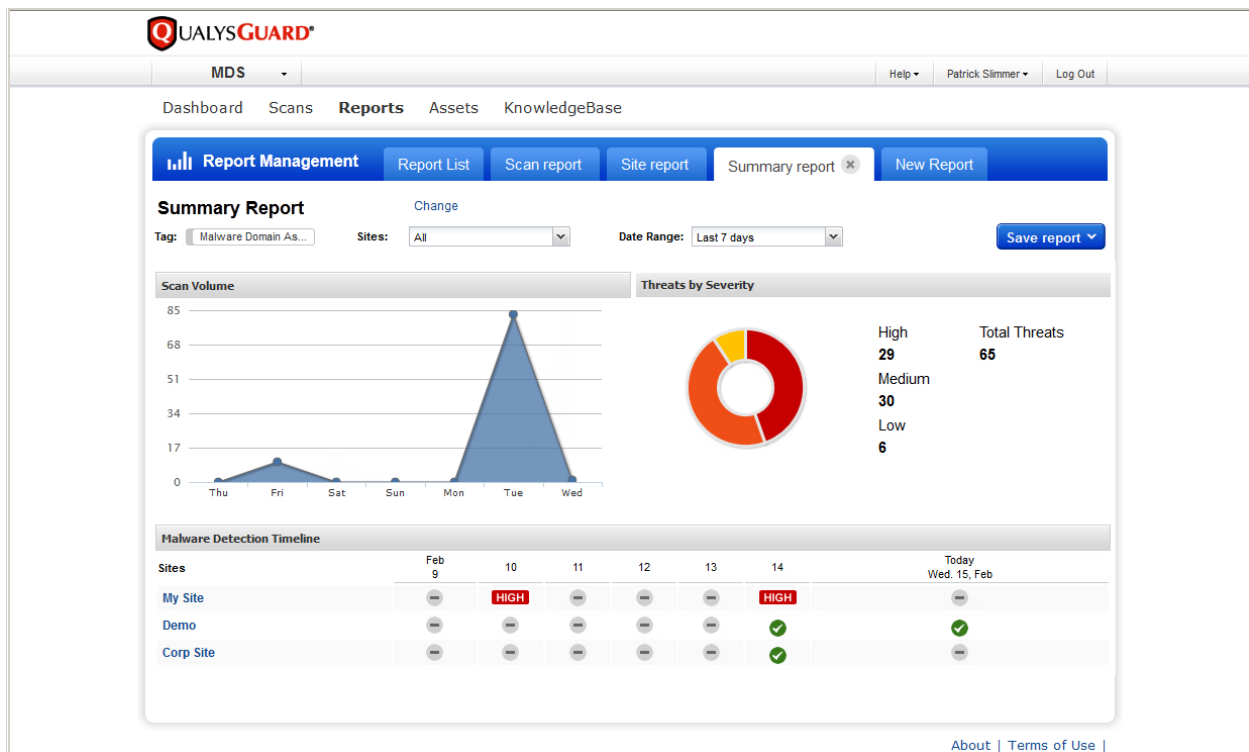
## Generate a New Report

Click the New Report tab to generate a new report. In the “Define your new report” window choose the type of report you want to create (Scan, Site or Summary) and select the information source for the report. The options that appear are specific to the selected report type. For a Scan Report, select a saved scan to report on. For a Site Report or Summary Report, choose a site by name or select a tag to report on all sites with the specified tag.

In the example on the next page, the user is generating a Summary Report based on all sites with the tag “Malware Domain Assets”.



Each report you generate opens on its own tab in the Report Management section. The service supports up to three open reports at one time. If you select New Report while you have three open reports, you will be prompted to save or delete the oldest report.



## Save the Report

After generating your report online click the “Save report” button to save the report to your account. You may save the report in one of these formats: ZIP, PDF and Encrypted PDF. When saving the report, you have the option to change the report name and add tags to the report. Users who have one or more of the applied tags assigned to their scope will be able to view and download the report. If saving the report in encrypted PDF format, you’ll also be prompted to provide a report password and an email distribution list for distributing your report. All saved reports appear on the Report List.

## View the Report List

The Report List is where you view saved reports. Saved reports appear here automatically. From this list you can download saved reports, add tags to reports, and send encrypted PDF reports to additional users.

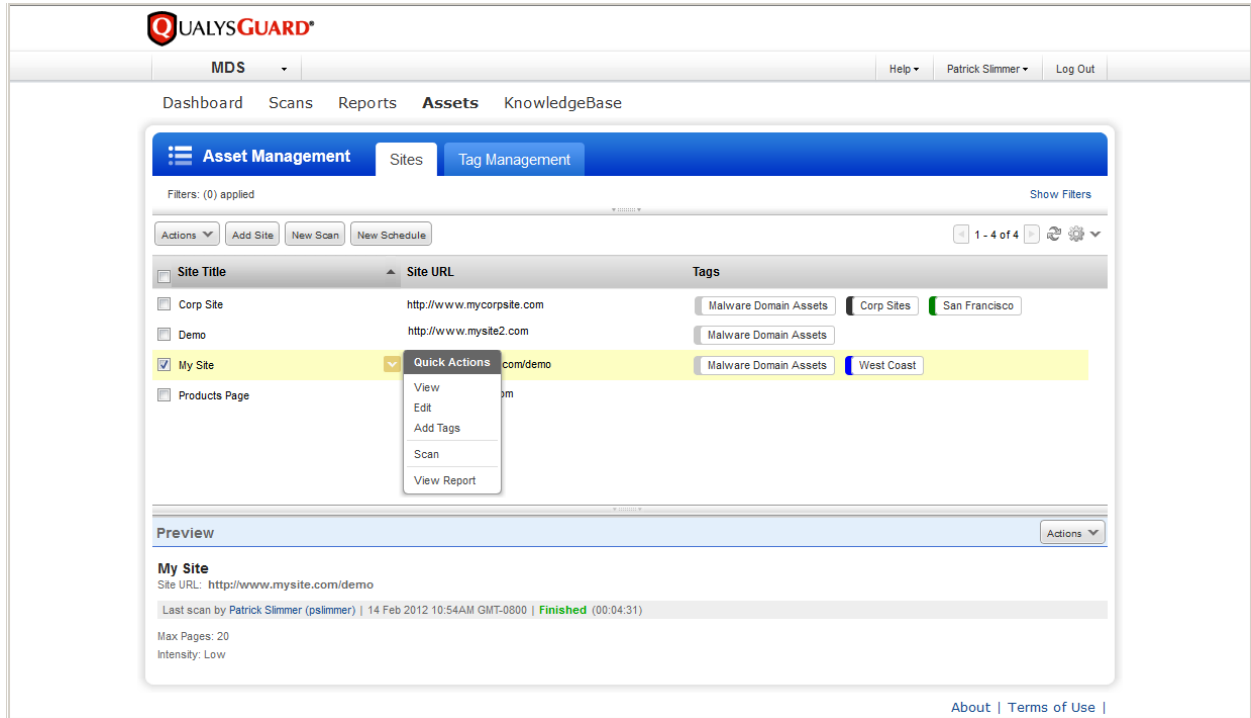
The screenshot displays the QualysGuard MDS interface. At the top, the 'QUALYS GUARD' logo is visible, followed by 'MDS' and user information 'Patrick Slimmer'. The main navigation includes 'Dashboard', 'Scans', 'Reports', 'Assets', and 'KnowledgeBase'. The 'Reports' section is active, showing 'Report Management' with tabs for 'Report List' and 'New Report'. Below this, there are filters and a table of reports.

Name	Format	Type	Status	Generation Date
<input type="checkbox"/> Summary Report	PDF (Encrypted)	Summary	Complete	14 Feb 2012
<input checked="" type="checkbox"/> Report on My Site (Feb 14)	Quick Actions	Site	Complete	14 Feb 2012
<input type="checkbox"/> Summary Report - Feb 6 to Feb 13	View	Summary	Complete	13 Feb 2012
<input type="checkbox"/> Scan Report - My Site	Download	Scan	Complete	13 Feb 2012
	Send Report			
	Add Tags			
	Delete			

Below the table is a 'Preview' section for the selected report 'Report on My Site (Feb 14)'. It shows the report type as 'Site Report', generated by Patrick Slimmer on 14 Feb 2012 at 9:47AM GMT-0800. The status is 'Complete' and it expires in 7 days. The format is 'Compressed HTML pages (ZIP)' and it has 1 download. Tags include 'West Coast' and 'Malware Domain Assets'.

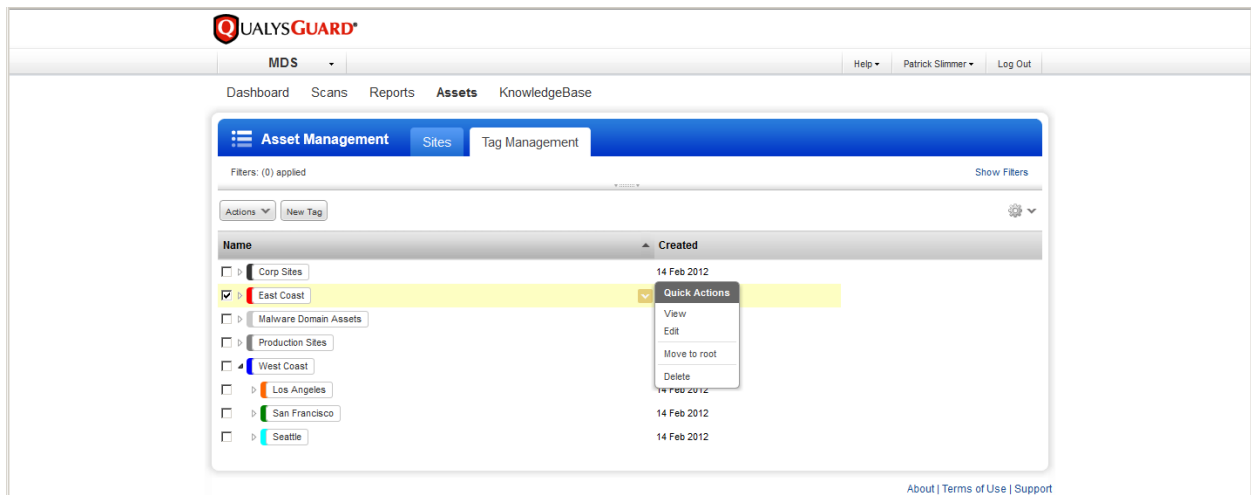
## Assets

Select Assets to go to the Asset Management section. This is where you add and manage the sites you want to scan for malware.



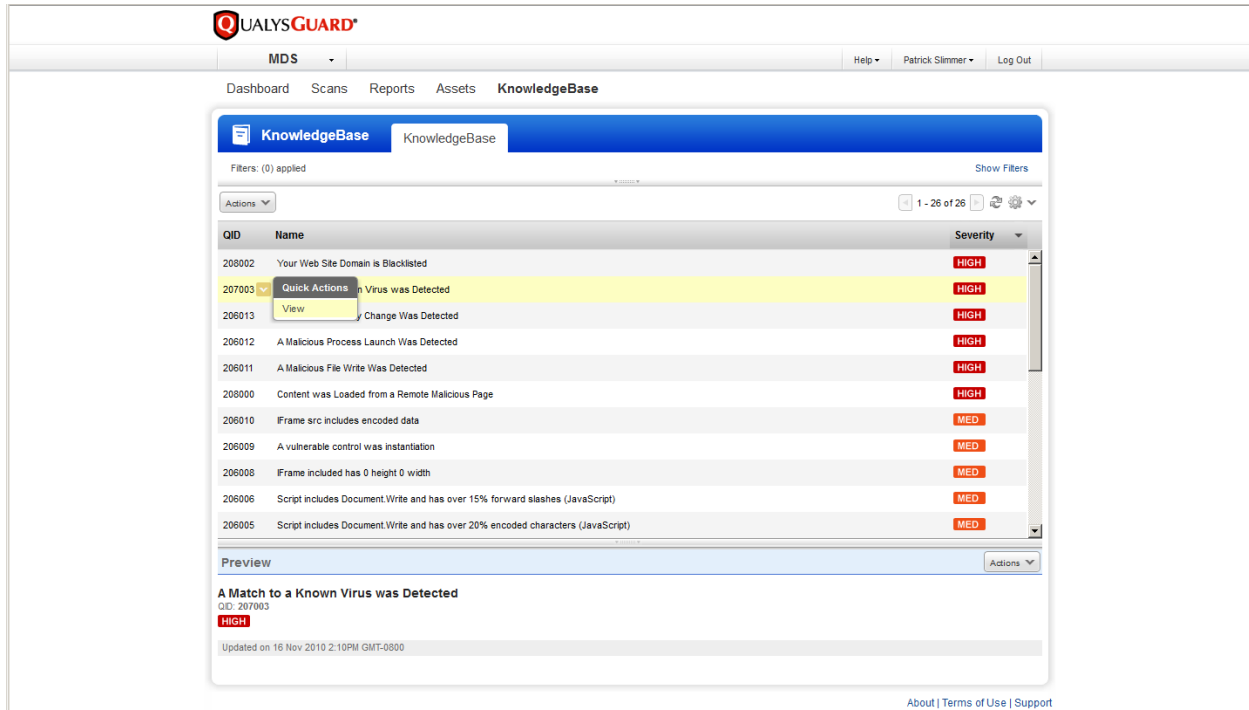
## Tag Management

The Tag Management tab under Assets is where you manage the tags that are used in your subscription to organize sites into meaningful categories. All tags in the subscription are listed. You can create tags that represent organizational groups (business units), geography (locations) or any other useful categorization. Tags can be applied to a site and used in reporting.



## KnowledgeBase

Select KnowledgeBase on the top menu to access the KnowledgeBase of QIDs detected by the service. Each QID is assigned a severity level (High, Medium, Low or Info) to help you prioritize remediation efforts. Click the Show Filters link to filter the list of QIDs based on severity level. To view details for a particular QID, select View from the Quick Actions menu.



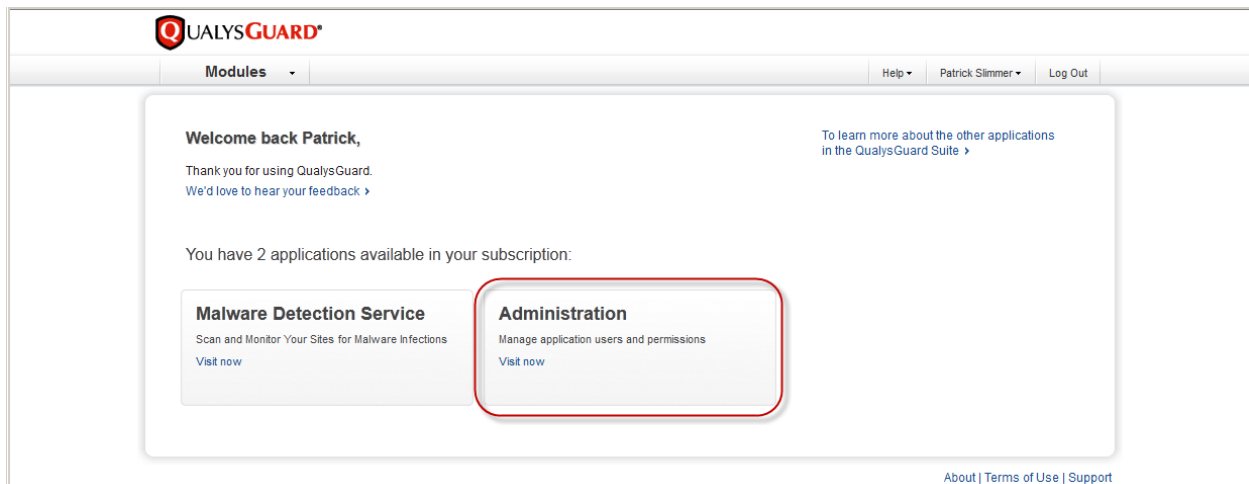
The screenshot shows the QualysGuard KnowledgeBase interface. At the top, there is a navigation bar with 'MDS' and user information. Below that, a breadcrumb trail shows 'Dashboard > Scans > Reports > Assets > KnowledgeBase'. The main content area has a 'KnowledgeBase' header and a table of QIDs. The table has columns for 'QID', 'Name', and 'Severity'. The QID 207003 is highlighted in yellow, and a 'Quick Actions' menu is open over it, showing a 'View' option. Below the table is a 'Preview' section for QID 207003, which shows a match to a known virus.

QID	Name	Severity
208002	Your Web Site Domain is Blacklisted	HIGH
207003	Virus was Detected	HIGH
206013	Change Was Detected	HIGH
206012	A Malicious Process Launch Was Detected	HIGH
206011	A Malicious File Write Was Detected	HIGH
208000	Content was Loaded from a Remote Malicious Page	HIGH
206010	Frame src includes encoded data	MED
206009	A vulnerable control was instantiation	MED
206008	Frame included has 0 height 0 width	MED
206006	Script includes Document.Write and has over 15% forward slashes (JavaScript)	MED
206005	Script includes Document.Write and has over 20% encoded characters (JavaScript)	MED

## Centralized Management

QualysGuard MDS Enterprise Edition supports multiple user accounts with user-defined roles and scopes. Create the roles you need to support your user base and assign appropriate permissions to each role.

Manage users using the Administration application.



The screenshot shows the QualysGuard Administration application interface. At the top, there is a navigation bar with 'Modules' and user information. The main content area has a welcome message for 'Patrick' and a link to learn more about other applications. Below that, there are two application tiles: 'Malware Detection Service' and 'Administration'. The 'Administration' tile is highlighted with a red border and contains the text 'Manage application users and permissions' and a 'Visit now' link.

In the Administration application, go to the User Management tab to see a list of users in your subscription. From here you can make changes to user account settings and create new users. Each user is assigned roles with permissions (what the user can do) and scopes (what the user can access).

The screenshot displays the QualysGuard User Management interface. At the top, the QualysGuard logo is visible, along with the user 'Admin' and navigation links for 'Help', 'Patrick Slimmer', and 'Log Out'. Below the header, there are tabs for 'Users' and 'Action Log'. The main content area is titled 'User Management' and contains a search bar, a 'Create User' button, and a table of users. The table has columns for 'Username', 'First Name', 'Last Name', and 'Email Address'. Two users are listed: 'noah' and 'pslimmer'. The 'pslimmer' user is selected, and a 'Quick Actions' menu is open over it, showing options for 'View', 'Edit', 'Delete', and 'Add Tags'. Below the table, there is a 'Preview' section for the selected user, 'Patrick Slimmer'. The preview shows the user's email as 'pslimmer@qualys.com', their last login date as '14 Feb 2012 3:16PM GMT-0800', and their status as 'Active'. It also lists their roles as 'All roles granted' and their tags as '-'. At the bottom right of the interface, there are links for 'About', 'Terms of Use', and 'Support'.

Username	First Name	Last Name	Email Address
<input type="checkbox"/> noah	Noah	Vail	nvail@qualys.com
<input checked="" type="checkbox"/> pslimmer		Slimmer	pslimmer@qualy...

**Patrick Slimmer**  
Email: pslimmer@qualys.com  
Username: pslimmer | Last logged in on 14 Feb 2012 3:16PM GMT-0800 | **Active**  
Roles: All roles granted  
Tags: -