Vulnerability Notification for Teams

Quick Start

November 20, 2017

Qualys, Inc.
919 E Hillsdale Blvd
Foster City, CA 94404
1 (650) 801 6100

Contents

Inform your teams on vulnerabilities

The Qualys KnowledgeBase has the largest and most up to date number of vulnerability tests available in the world. By setting up the vulnerability notification feature your teams will be informed on vulnerabilities they are interested in - new and updated vulnerabilities will be included.

Start sending notifications to your teams

Create new users (optional). Vulnerability notifications can be sent to existing users in your subscription and to users outside of the subscription. Notifications may also be sent to KnowledgeBase Only users when this option is enabled for your subscription.

Associate users with vulnerabilities. Create search lists to identify vulnerabilities your teams will be alerted on, and assign them (and users) to distribution groups.

We'll start sending notifications to users! Your users will receive notifications on the vulnerabilities that match search lists in distribution groups they are assigned to.

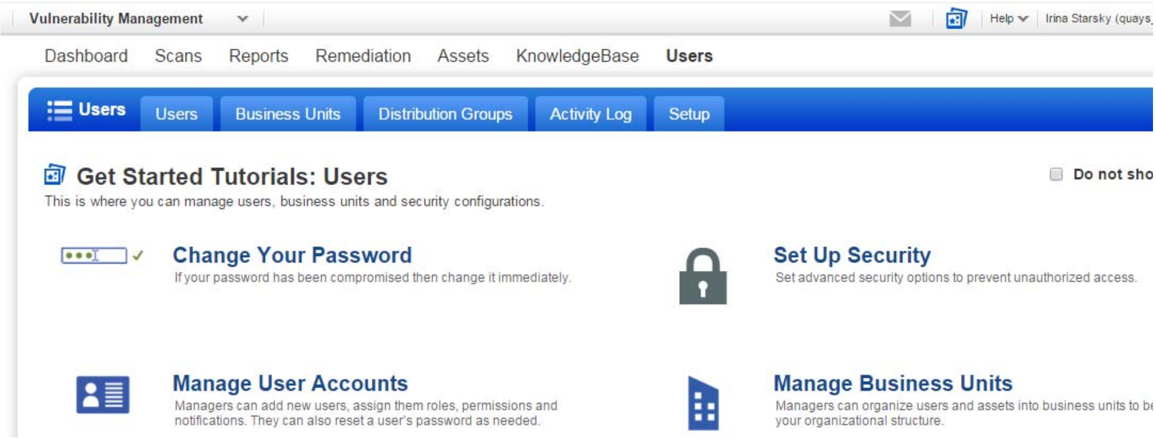
Tell me about KnowledgeBase Only users

- KnowledgeBase Only is a user role with limited access to the UI. This user role is available only when enabled for your subscription. Don't have this? Contact your Technical Account Manager or our Support Team.

- KnowledgeBase Only users can send and receive vulnerability notifications, and view vulnerabilities in the Qualys KnowledgeBase. They are in the Unassigned business unit and do not have any assets.

How do I create users with KnowledgeBase Only access

You'll create new users from the Users section.



Get Started Tutorials: Users

This is where you can manage users, business units and security configurations.

Change Your Password

If your password has been compromised then change it immediately.

Set Up Security

Set advanced security options to prevent unauthorized access.

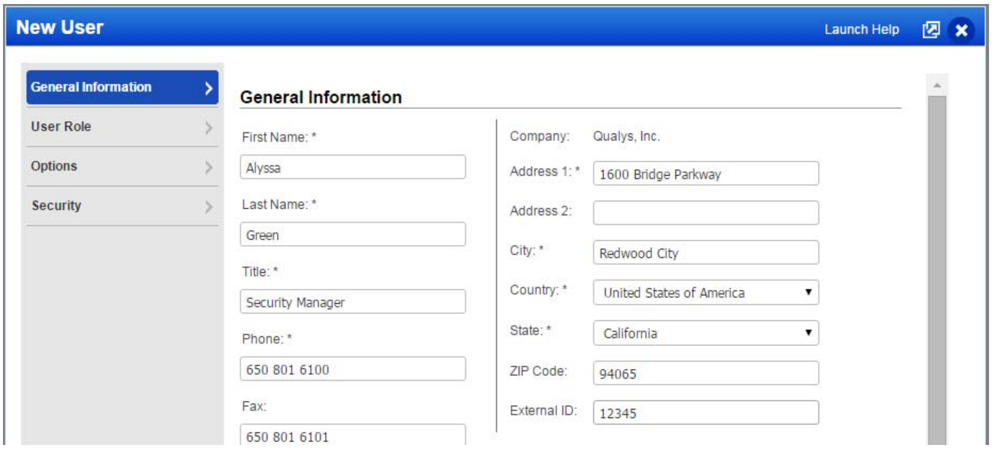
Manage User Accounts

Managers can add new users, assign them roles, permissions and notifications. They can also reset a user's password as needed.

Manage Business Units

Managers can organize users and assets into business units to be your organizational structure.

Go to the Users tab and select New > User and enter user information like any other user.



General Information

First Name: * Alyssa

Last Name: * Green

Title: * Security Manager

Phone: * 650 801 6100

Fax: 650 801 6101

Company: Qualys, Inc.

Address 1: * 1600 Bridge Parkway

Address 2:

City: * Redwood City

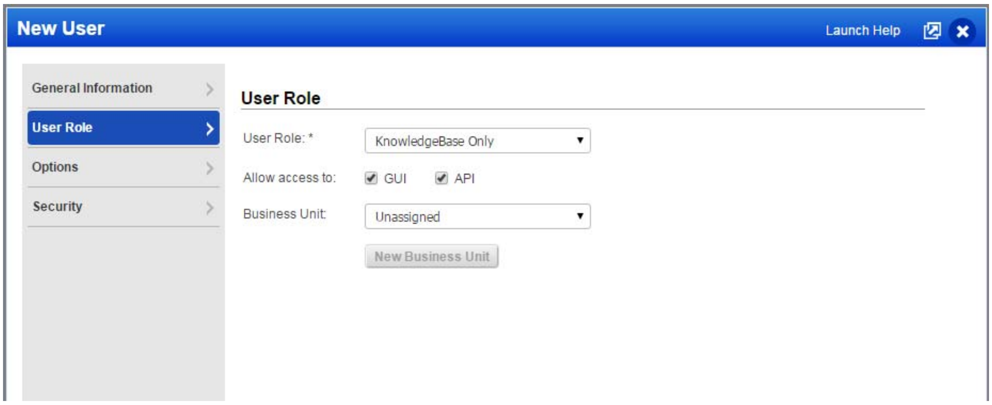
Country: * United States of America ▾

State: * California ▾

ZIP Code: 94065

External ID: 12345

For user role select “KnowledgeBase Only”. You’ll notice this user is not assigned any assets.



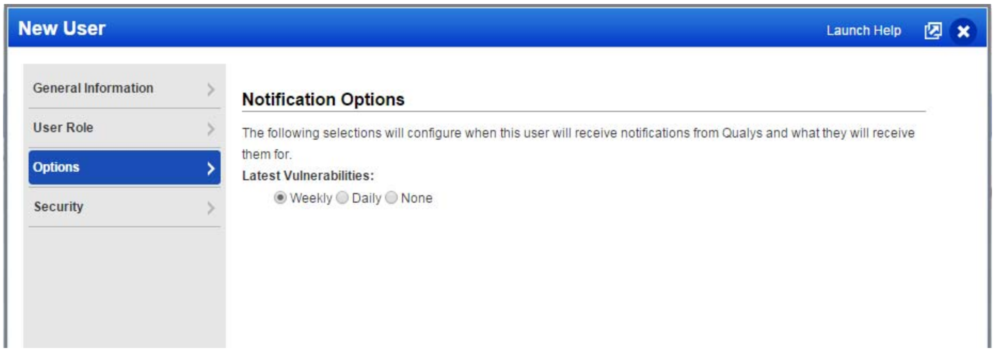
User Role

User Role: * KnowledgeBase Only ▾

Allow access to: ☑ GUI ☑ API

Business Unit: Unassigned ▾

By default the user will receive the Latest Vulnerabilities notification on a weekly basis. This email lists all vulnerabilities and potential vulnerabilities added to the Qualys KnowledgeBase since the previous week. You can change the email frequency to daily or turn it off.



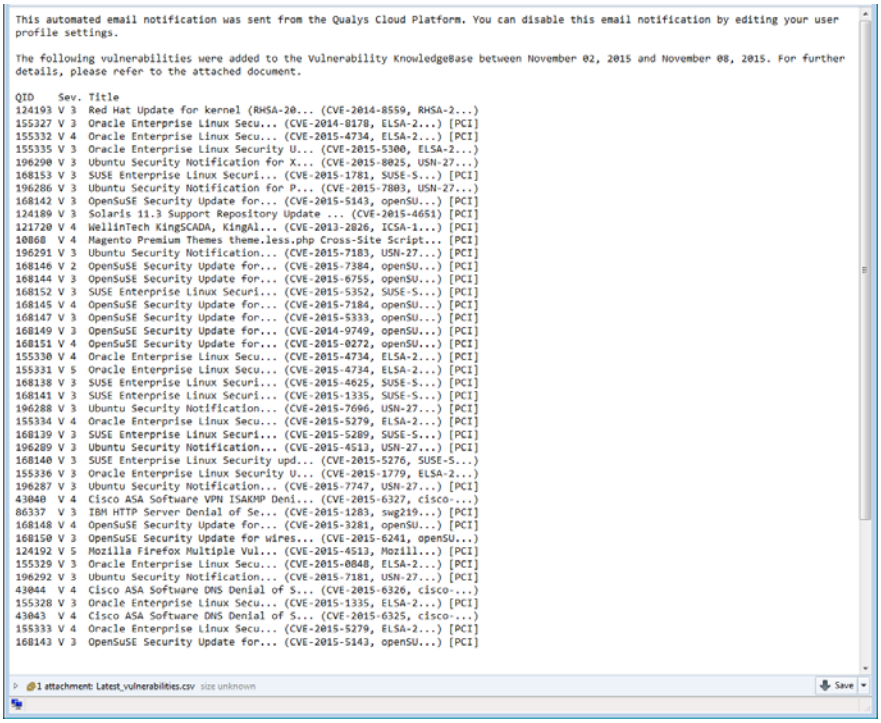
Notification Options

The following selections will configure when this user will receive notifications from Qualys and what they will receive them for.

Latest Vulnerabilities:

● Weekly ○ Daily ○ None

This sample Latest Vulnerabilities notification shows vulnerabilities added between November 2, 2015 and November 8, 2015. A CSV file is attached to provide additional details for each QID.



```
This automated email notification was sent from the Qualys Cloud Platform. You can disable this email notification by editing your user
profile settings.

The following vulnerabilities were added to the Vulnerability KnowledgeBase between November 02, 2015 and November 08, 2015. For further
details, please refer to the attached document.

QID    Sev. Title
124193 V 3  Red Hat Update for kernel (RHSA-20... (CVE-2014-8559, RHSA-2...)
155327 V 3  Oracle Enterprise Linux Secu... (CVE-2014-8178, ELSA-2...) [PCI]
155332 V 4  Oracle Enterprise Linux Secu... (CVE-2015-4734, ELSA-2...) [PCI]
155335 V 3  Oracle Enterprise Linux Security U... (CVE-2015-5300, ELSA-2...)
196290 V 3  Ubuntu Security Notification for X... (CVE-2015-8025, USN-27...)
168153 V 3  SUSE Enterprise Linux Securi... (CVE-2015-1781, SUSE-S...) [PCI]
196286 V 3  Ubuntu Security Notification for P... (CVE-2015-7803, USN-27...)
168142 V 3  OpenSuSE Security Update for... (CVE-2015-5143, openSU...) [PCI]
124189 V 3  Solaris 11.3 Support Repository Update ... (CVE-2015-4651) [PCI]
121720 V 4  WellinTech KingSCADA, KingAl... (CVE-2013-2826, ICSA-1...) [PCI]
10868  V 4  Magento Premium Themes theme.less.php Cross-Site Script... [PCI]
196291 V 3  Ubuntu Security Notification... (CVE-2015-7183, USN-27...) [PCI]
168146 V 2  OpenSuSE Security Update for... (CVE-2015-7384, openSU...) [PCI]
168144 V 3  OpenSuSE Security Update for... (CVE-2015-6755, openSU...) [PCI]
168152 V 3  SUSE Enterprise Linux Securi... (CVE-2015-5352, SUSE-S...) [PCI]
168145 V 4  OpenSuSE Security Update for... (CVE-2015-7184, openSU...) [PCI]
168147 V 3  OpenSuSE Security Update for... (CVE-2015-5333, openSU...) [PCI]
168149 V 3  OpenSuSE Security Update for... (CVE-2014-9749, openSU...) [PCI]
168151 V 4  OpenSuSE Security Update for... (CVE-2015-0272, openSU...) [PCI]
155330 V 4  Oracle Enterprise Linux Secu... (CVE-2015-4734, ELSA-2...) [PCI]
155331 V 5  Oracle Enterprise Linux Secu... (CVE-2015-4734, ELSA-2...) [PCI]
168138 V 3  SUSE Enterprise Linux Securi... (CVE-2015-4625, SUSE-S...) [PCI]
168141 V 3  SUSE Enterprise Linux Securi... (CVE-2015-1335, SUSE-S...) [PCI]
196288 V 3  Ubuntu Security Notification... (CVE-2015-7696, USN-27...) [PCI]
155334 V 4  Oracle Enterprise Linux Secu... (CVE-2015-5279, ELSA-2...) [PCI]
168139 V 3  SUSE Enterprise Linux Securi... (CVE-2015-5289, SUSE-S...) [PCI]
196289 V 3  Ubuntu Security Notification... (CVE-2015-4513, USN-27...) [PCI]
168140 V 3  SUSE Enterprise Linux Security upd... (CVE-2015-5276, SUSE-S...)
155336 V 3  Oracle Enterprise Linux Security U... (CVE-2015-1779, ELSA-2...)
196287 V 3  Ubuntu Security Notification... (CVE-2015-7747, USN-27...) [PCI]
43040  V 4  Cisco ASA Software VPN ISAKMP Deni... (CVE-2015-6327, cisco-...)
86337  V 3  IBM HTTP Server Denial of Se... (CVE-2015-1283, swg219...) [PCI]
168148 V 4  OpenSuSE Security Update for... (CVE-2015-3281, openSU...) [PCI]
168150 V 3  OpenSuSE Security Update for wires... (CVE-2015-6241, openSU...)
124192 V 5  Mozilla Firefox Multiple Vul... (CVE-2015-4513, Mozill...) [PCI]
155329 V 3  Oracle Enterprise Linux Secu... (CVE-2015-0848, ELSA-2...) [PCI]
196292 V 3  Ubuntu Security Notification... (CVE-2015-7181, USN-27...) [PCI]
43044  V 4  Cisco ASA Software DNS Denial of S... (CVE-2015-6326, cisco-...)
155328 V 3  Oracle Enterprise Linux Secu... (CVE-2015-1335, ELSA-2...) [PCI]
43043  V 4  Cisco ASA Software DNS Denial of S... (CVE-2015-6325, cisco-...)
155333 V 4  Oracle Enterprise Linux Secu... (CVE-2015-5279, ELSA-2...) [PCI]
168143 V 3  OpenSuSE Security Update for... (CVE-2015-5143, openSU...) [PCI]
```

1 attachment: Latest_vulnerabilities.csv size unknown

User creation using the API

Our Qualys API supports adding KnowledgeBase Only users. The User API v1 (/msp/user.php) can be used to create users using the parameter **`user_role=kbuser`**.

Sample API request

This request creates a new KnowledgeBase Only user including all required parameters:

```
https://qualysapi.qualys.com/msp/user.php?action=add&user_role=kbuser&bu
siness_unit=Unassigned&first_name=Jason&last_name=Kim&title=Security+Con
sultant&phone=2126667777&email=jason@mycompany.com&address1=500+Charles_
Avenue&city=New+York&country=United+States+of+America&state=New+York
```

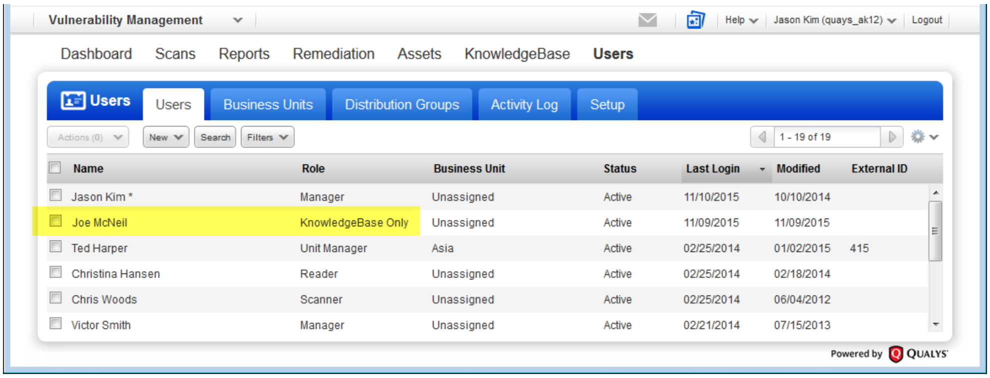
(where “qualysapi.qualys.com” is the platform URL associated with the API user’s account)

Each new user receives their login credentials and instructions via email

All the user has to do is login to complete their account registration. After this the user is activated and ready to receive vulnerability email notifications you set up for them.

New users are added to your account

You'll see KnowledgeBase Only users listed with other users in your account.



Name	Role	Business Unit	Status	Last Login	Modified	External ID
Jason Kim *	Manager	Unassigned	Active	11/10/2015	10/10/2014	
Joe McNeil	KnowledgeBase Only	Unassigned	Active	11/09/2015	11/09/2015	
Ted Harper	Unit Manager	Asia	Active	02/25/2014	01/02/2015	415
Christina Hansen	Reader	Unassigned	Active	02/25/2014	02/18/2014	
Chris Woods	Scanner	Unassigned	Active	02/25/2014	06/04/2012	
Victor Smith	Manager	Unassigned	Active	02/21/2014	07/15/2013	

How do I create custom notifications

It's easy to configure different vulnerability notifications for different teams. For example, you may want a group of IT Managers tasked with maintaining Windows systems to be notified when new critical Microsoft vulnerabilities are added to the KnowledgeBase. You may want a separate group responsible for monitoring cyber threats to be notified about all vulnerabilities with known exploits so they can be proactive and take appropriate actions even before a scan is launched.

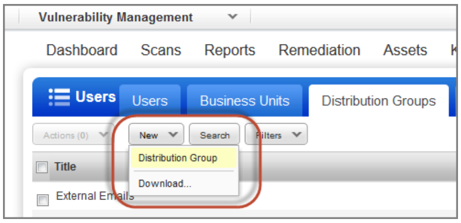
Who can do this?

Manager users and KnowledgeBase Only users can set up custom vulnerability notifications.

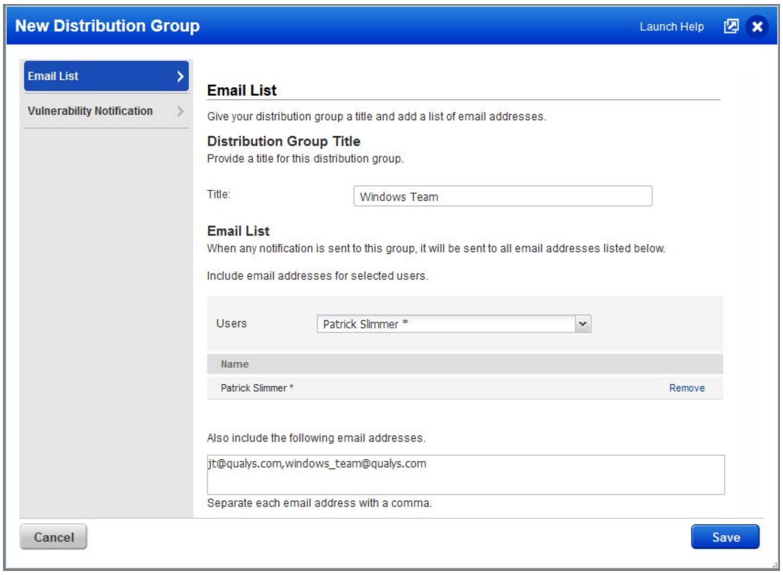
Let's get started!

You'll create distribution groups with 1) users and 2) search lists that tell us which vulnerabilities those users should be informed about. When a vulnerability (QID) matches the search list, the entire distribution group is notified by email.

Go to Users > Distribution Groups, and choose New > Distribution Group.



Give your distribution group a name and add the list of users who are members of the group.



Email List

Give your distribution group a title and add a list of email addresses.

Distribution Group Title

Provide a title for this distribution group.

Title: Windows Team

Email List

When any notification is sent to this group, it will be sent to all email addresses listed below.

Include email addresses for selected users.

Users: Patrick Slimmer *

Name	
Patrick Slimmer *	Remove

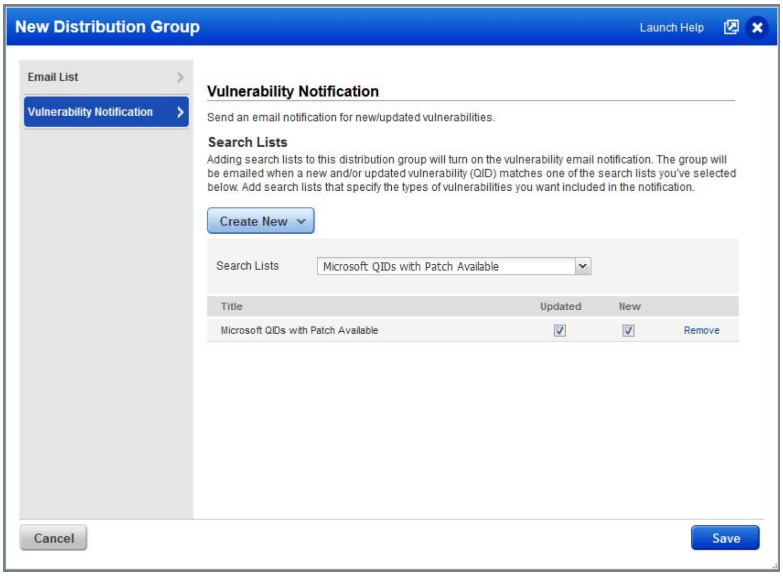
Also include the following email addresses.

jt@qualys.com,windows_team@qualys.com

Separate each email address with a comma.

Include email addresses for users in the subscription (simply select users from the list) and email addresses for users outside of the subscription (type them into the field provided).

Select vulnerabilities that will trigger emails. Use search lists to tell us which vulnerabilities should result in an email notification for this particular distribution group.



Vulnerability Notification

Send an email notification for new/updated vulnerabilities.

Search Lists

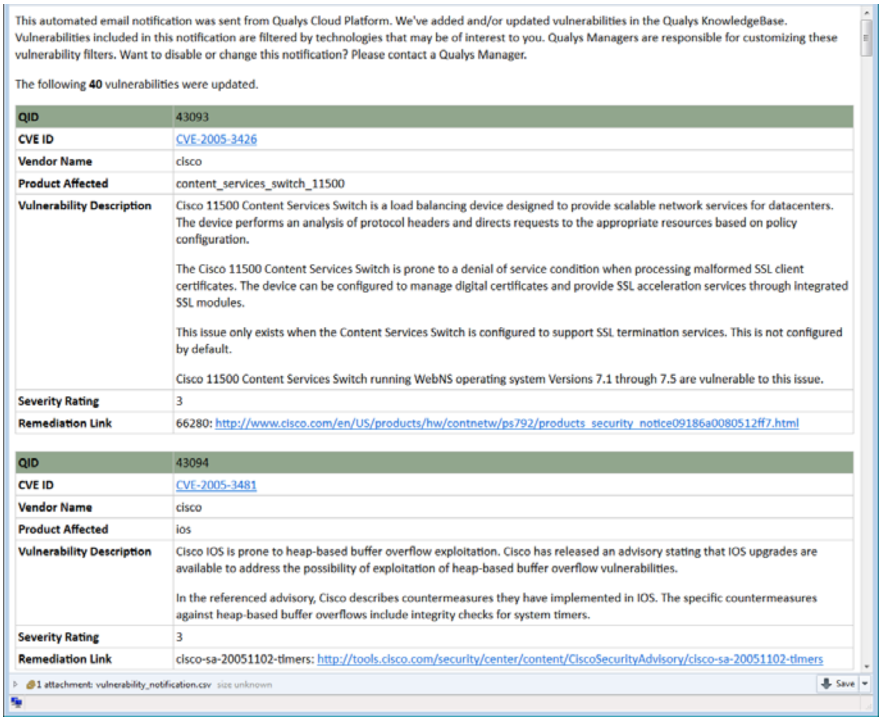
Adding search lists to this distribution group will turn on the vulnerability email notification. The group will be emailed when a new and/or updated vulnerability (QID) matches one of the search lists you've selected below. Add search lists that specify the types of vulnerabilities you want included in the notification.

Search Lists: Microsoft QIDs with Patch Available

Title	Updated	New	
Microsoft QIDs with Patch Available	☑	☑	Remove

Configure the notification to be sent for new vulnerabilities, updated vulnerabilities or both.

Here’s a sample notification. A CSV file is attached to provide additional details for each QID.



This automated email notification was sent from Qualys Cloud Platform. We've added and/or updated vulnerabilities in the Qualys KnowledgeBase. Vulnerabilities included in this notification are filtered by technologies that may be of interest to you. Qualys Managers are responsible for customizing these vulnerability filters. Want to disable or change this notification? Please contact a Qualys Manager.

The following **40** vulnerabilities were updated.

QID	43093
CVE ID	CVE-2005-3426
Vendor Name	cisco
Product Affected	content_services_switch_11500
Vulnerability Description	Cisco 11500 Content Services Switch is a load balancing device designed to provide scalable network services for datacenters. The device performs an analysis of protocol headers and directs requests to the appropriate resources based on policy configuration. The Cisco 11500 Content Services Switch is prone to a denial of service condition when processing malformed SSL client certificates. The device can be configured to manage digital certificates and provide SSL acceleration services through integrated SSL modules. This issue only exists when the Content Services Switch is configured to support SSL termination services. This is not configured by default. Cisco 11500 Content Services Switch running WebNS operating system Versions 7.1 through 7.5 are vulnerable to this issue.
Severity Rating	3
Remediation Link	66280: http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_security_notice09186a0080512ff7.html

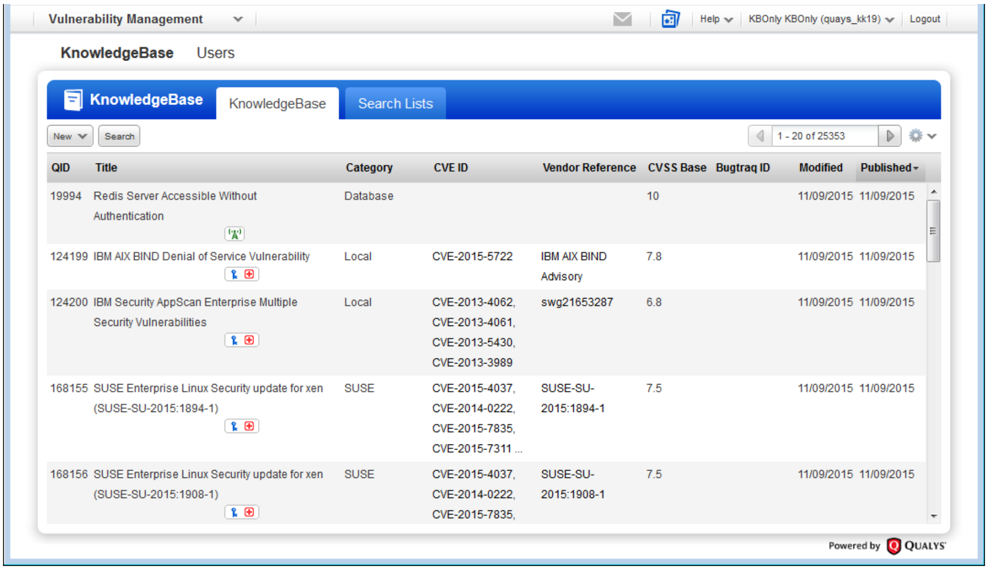
QID	43094
CVE ID	CVE-2005-3481
Vendor Name	cisco
Product Affected	ios
Vulnerability Description	Cisco IOS is prone to heap-based buffer overflow exploitation. Cisco has released an advisory stating that IOS upgrades are available to address the possibility of exploitation of heap-based buffer overflow vulnerabilities. In the referenced advisory, Cisco describes countermeasures they have implemented in IOS. The specific countermeasures against heap-based buffer overflows include integrity checks for system timers.
Severity Rating	3
Remediation Link	cisco-sa-20051102-timers: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers

How users stay updated on vulnerabilities

Users are able to send and receive vulnerability notifications, and view vulnerabilities in the KnowledgeBase.

View vulnerabilities in the KnowledgeBase

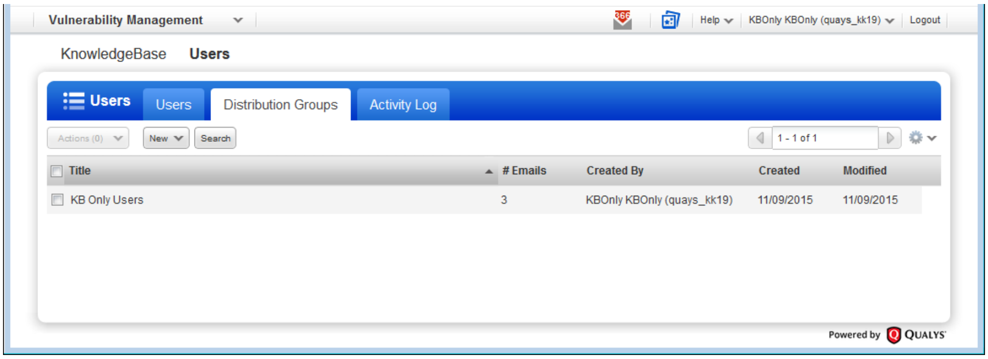
Search the KnowledgeBase, dig into vulnerability details, and create search lists (on the Search Lists tab). You'll need search lists for custom vulnerability notifications. The KnowledgeBase is the default landing page for KnowledgeBase Only users.



QID	Title	Category	CVE ID	Vendor Reference	CVSS Base	Bugtraq ID	Modified	Published
19994	Redis Server Accessible Without Authentication	Database			10		11/09/2015	11/09/2015
124199	IBM AIX BIND Denial of Service Vulnerability	Local	CVE-2015-5722	IBM AIX BIND Advisory	7.8		11/09/2015	11/09/2015
124200	IBM Security AppScan Enterprise Multiple Security Vulnerabilities	Local	CVE-2013-4062, CVE-2013-4061, CVE-2013-5430, CVE-2013-3989	swg21653287	6.8		11/09/2015	11/09/2015
168155	SUSE Enterprise Linux Security update for xen (SUSE-SU-2015:1894-1)	SUSE	CVE-2015-4037, CVE-2014-0222, CVE-2015-7835, CVE-2015-7311 ...	SUSE-SU-2015:1894-1	7.5		11/09/2015	11/09/2015
168156	SUSE Enterprise Linux Security update for xen (SUSE-SU-2015:1908-1)	SUSE	CVE-2015-4037, CVE-2014-0222, CVE-2015-7835,	SUSE-SU-2015:1908-1	7.5		11/09/2015	11/09/2015

Set up custom vulnerability notifications

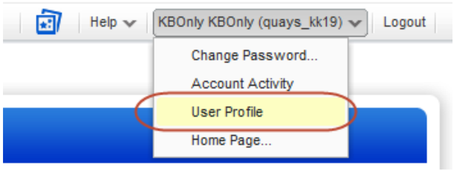
Jump over to the Users section to create distribution groups and set up your own custom vulnerability notifications. It's easy to do. Go here for step-by-step instructions.



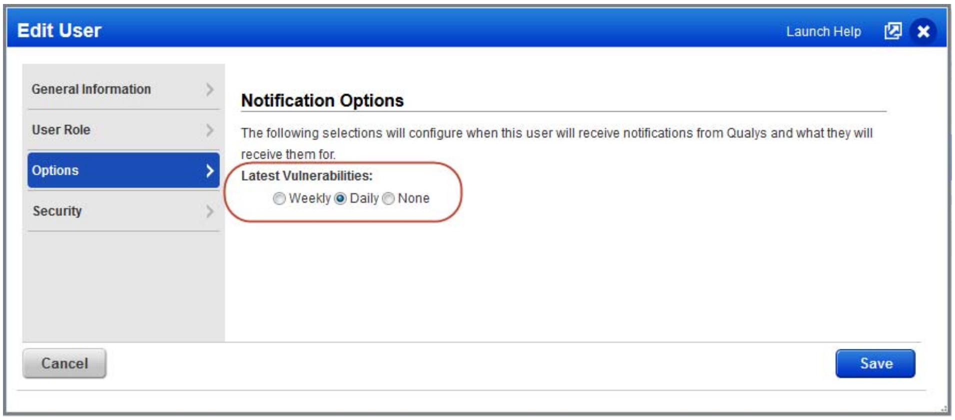
□ Title	# Emails	Created By	Created	Modified
□ KB Only Users	3	KBOnly KBOnly (quays_kk19)	11/09/2015	11/09/2015

Configure the Latest Vulnerabilities notification

This email notification is sent weekly, by default. Would you prefer to receive it daily or not at all? Simply choose User Profile below your user name (in the top right corner).



Then go to the Options section to change the notification setting for your account.



Notification Options

The following selections will configure when this user will receive notifications from Qualys and what they will receive them for.

Latest Vulnerabilities:
○ Weekly ● Daily ○ None

User permissions and controls

Tell me about user permissions

KnowledgeBase Only users have these permissions:

Can edit their own user profile.

Can view the Qualys KnowledgeBase.

Can create Search Lists and edit or delete their own Search Lists.

Cannot create or edit global Search Lists.

Can create Distribution Groups and edit or delete their own Distribution Groups.

Idefense and Predictions tabs will be shown when enabled.

Can run basic APIs when enabled in the UI.

Basic API support

APIv1

1) /msp/time_zone_code_list.php

2) /msp/scan_options.php

3) /msp/ticket_list.php

4) /msp/asset_ip_list.php

5) /msp/asset_domain_list.php

6) /msp/action_log_report.php

APIv2

1) /api/2.0/fo/scan/

2) /api/2.0/fo/report/scorecard/ (launch scorecard report)

3) /api/2.0/fo/asset/ip/

4) /api/2.0/fo/asset/excluded_ip/?action=list&echo_request=0

5) /api/2.0/fo/asset/group/

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Fujitsu, HCL Comnet, HPE, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys 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 support information at www.qualys.com/support/