CISCO
SECURE

Kenna Getting Started Guide

version 1.0

February 2022

The bridge to possible

Contents

Document History

Issue Month	Version	Comments
December, 2021	Pre-Release	First Draft
January, 2022	Pre-Release	Review by the CX & Product Marketing Teams
February, 2022	Pre-Release	Review by the Product Management Team
February, 2022	Version 1.0	Approved version

Purpose

Implementing a platform like Kenna Security that offers so much in terms of value and functionality can be a truly daunting task. Even with training and an abundance of help articles that are publicly available, having a rounded understanding of the platform can still feel elusive. This document aims to serve as a guide to introduce concepts that are fundamental to working in the platform, as well as instructions for carrying out some common tasks and activities in Kenna. As much as possible, topics build on already covered ideas and so should be of great value to a person who has minimal exposure to the Kenna platform. For individuals already familiar with Kenna, it can still serve as a reference to review a forgotten concept, or how a particular task is done.

Items to be covered in this documentation include the following:

a. Overview of the Kenna platform - Dashboard, Explore, AppSec, VI, Settings

b. Common Concepts – Asset Statuses in Kenna, Vulnerability Statuses in Kenna, Risk Meters / Asset Searches, Asset prioritization, Scoring in Kenna - Vulnerability score, Asset Score, Risk Meter Score

c. Common Operations within Kenna
   - ✓ Viewing Assets
   - ✓ Viewing vulnerabilities
   - ✓ Viewing Risk Meters
   - ✓ Deep dive into Risk Meters / Asset searches

d. Settings page

e. API operations

Overview of the Kenna Platform Interface

Based on the actual configuration setup by administrators of the platform, a logged-on user will immediately see the Home Page (Figure 1.1), or the Vulnerability Explore page (Figure 1.2). The main UI elements of each page have been highlighted and explained.

Home Page Layout (Figure 1.1)

1. Home Page shortcut – Use this to access the Home Page at any time (if user has access to view it).
2. VM menu shortcut – Has menu options for the Dashboard and Explore pages.
3. AppSec menu shortcut – Has menu options for the AppSec Dashboard and Reporting pages.
4. VI menu shortcut – Has menu options to the VI product portal.
5. Connectors – Available to only administrators. This is used for setting up and managing data ingestion into Kenna.
6. Notifications – Any in-app notifications can be found here.
7. Settings – Shows name of environment and provides access to the settings available to the user.
8. Site-wide metrics – Indicates metrics for the entire site.
9. Connector runs – Provides indication of the status of last five connector runs for the platform.

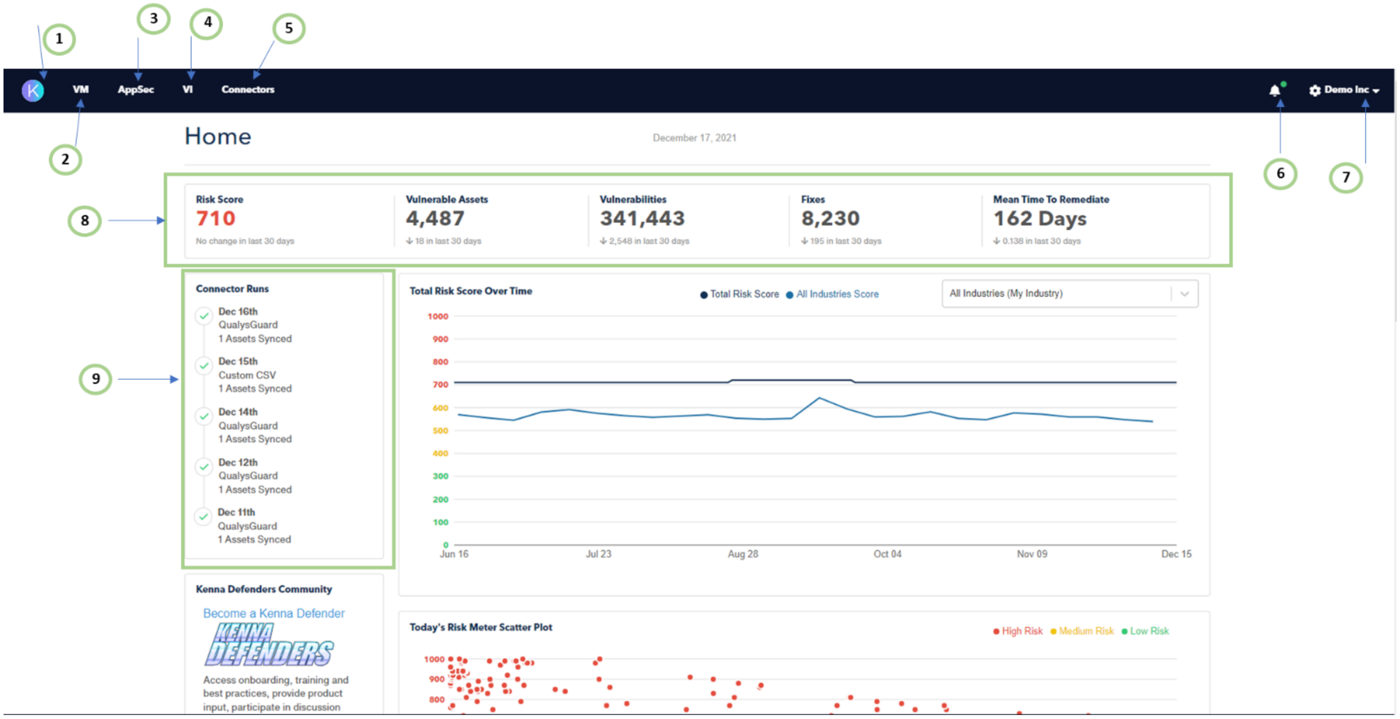


Figure 1.1 – Layout of the Home Page

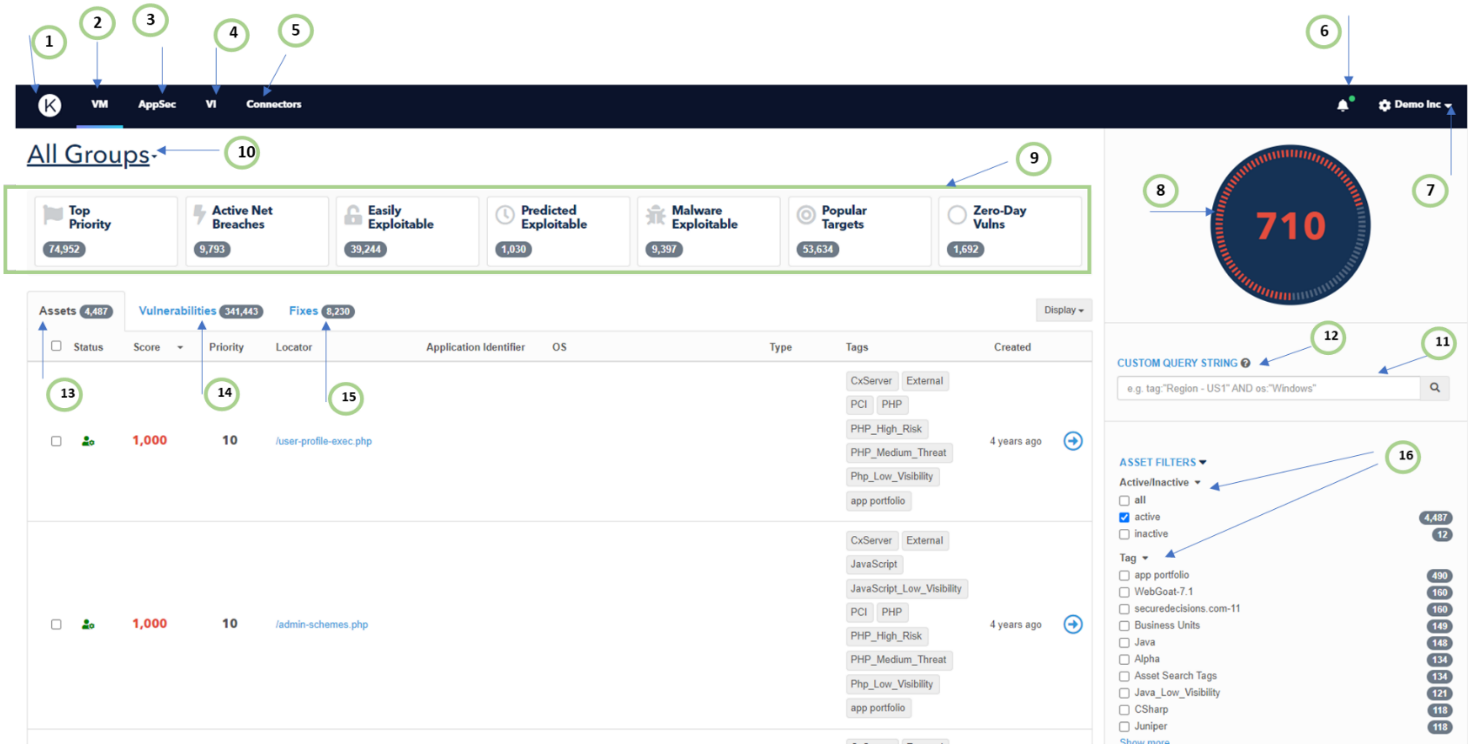


Figure 1.2 – Layout of the Default Explore Page

Default Explore Page Layout (Figure 1.2)

1. Home Page shortcut – Use this to access the Home Page at any time (if user has access to view it).
2. VM menu shortcut – Has menu options for the Dashboard and Explore pages.
3. AppSec menu shortcut – Has menu options for the AppSec Dashboard and Reporting pages.
4. VI menu shortcut – Has menu options to the VI product portal.
5. Connectors – Available to only administrators. This is used for setting up and managing data ingestion into Kenna.
6. Notifications – Any in-app notifications can be found here.
7. Settings – Shows name of environment and provides access to the settings available to the user.
8. Risk Meter score – Shows risk score of the group of Assets from the search bar. Default shown is 'All Assets' Risk Meter.
9. Useful Vuln Categories – Provides useful filters (assets and vulnerabilities) to return a subset of assets in an environment.
10. Risk Meter Selection / Search – Used to search and select Risk Meters in the VM Explore page.
11. Query Builder – Used for flexible searching of assets and vulnerabilities.
12. Custom Query String Help – Help page to provide guidance on how to build queries for asset searches.
13. Assets Tab – Provides a view for all your assets. This is the default view in the Explore page
14. Vulnerabilities Tab – Provides a view of all your vulnerabilities.
15. Fixes Tab – Provides access to all the Fixes in a particular environment / view.
16. Filters – These asset and vulnerability filters can be used as quick selections to return a subset of an organizations' data.

Common Concepts in Kenna

The following concepts will be discussed:

- Asset Statuses in Kenna
- Vulnerability Statuses in Kenna
- Risk Meter/Asset Searches
- Asset prioritization
- Scoring in Kenna – Vulnerability / Risk Score, Asset Score and Risk Meter Score

Asset Statuses in Kenna

Assets within Kenna are the configuration items for an organization, ingested into Kenna through one or multiple connectors. Each asset can have 0 or more vulnerabilities on it which are tracked and reported on the Kenna platform. An asset within Kenna can have a status of Active or Inactive. Kenna automatically manages the status of assets using a preconfigured asset inactivity setting in the Settings page. This page is only available to administrators. Active assets represent assets that have been 'seen' from a connector within the time threshold of the asset inactivity setting. By default, only active assets are included in the calculation of a Risk Meter score. This default behavior can be changed using custom query strings, or asset and/or vulnerability filters.

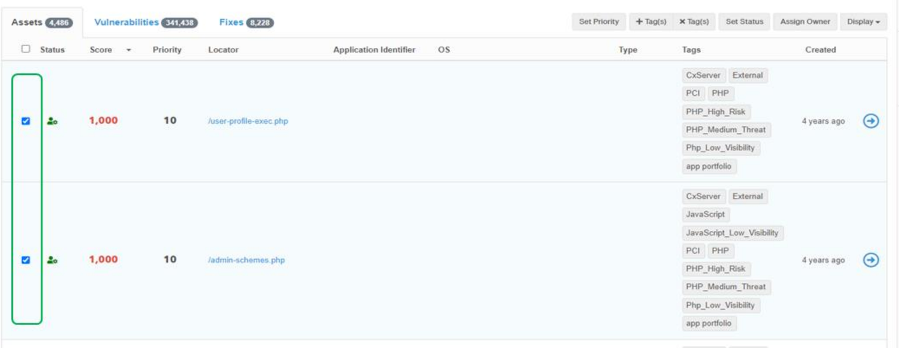
Once an asset exceeds the threshold set up in the asset inactivity setting, that asset becomes inactive, and no longer appears in the calculations for any Risk Meter that uses the default settings. If that inactive asset is part of another connector run, the asset status will be changed back to Active. If however, such inactive assets are not seen before yet another time setting elapses (purge setting), those assets are purged from the Kenna platform and Kenna no longer tracks those assets. If the asset is re-introduced at this point, the asset is treated as a new asset.

In summary:

- An active asset becomes inactive when the last seen time of that asset is greater than inactive asset setting
- An inactive asset becomes purged when the last seen time is greater than the asset purge setting

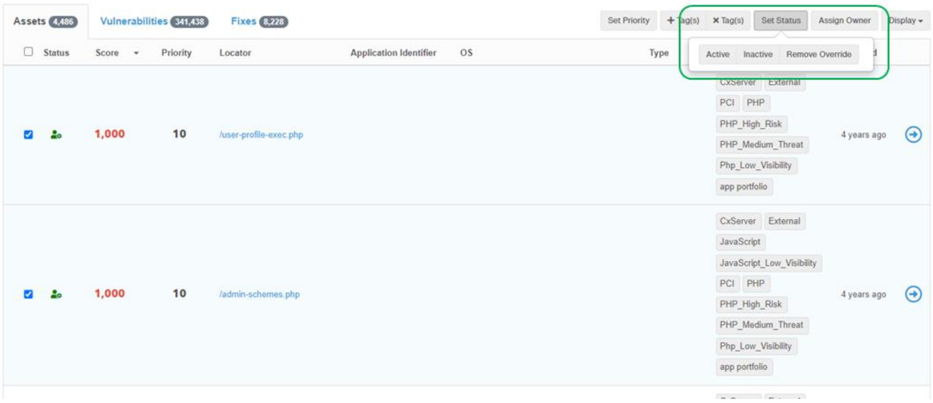
While Kenna automatically manages the status of assets as captured by the workflow above, users can set this status manually. Using the UI, the asset status can be modified for one or more assets.

Select one or more assets in Kenna by checking them as shown.



☐	Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
☑		1,000	10	/user-profile-exec.php				CxServer External PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☑		1,000	10	/admin-schemes.php				CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago

Click on 'Set Status', and from the resulting status options, modify the status of the asset as desired.



☐	Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	d
☑		1,000	10	/user-profile-exec.php				CxServer External PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☑		1,000	10	/admin-schemes.php				CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago

Note that Kenna would cease to manage the status of that asset once it has been manually changed. To transfer control of the asset back to Kenna, click on the ‘Remove Override’ button shown in the preceding image.

Vulnerabilities and Vulnerability Statuses

Similar to asset status, vulnerabilities within Kenna can have one of several statuses.

Open: These vulnerabilities are currently being reported within Kenna as open, and as long as a score is present, will potentially affect the asset score of its asset. See the ‘Scoring in Kenna’ section for details of how asset scoring is done.

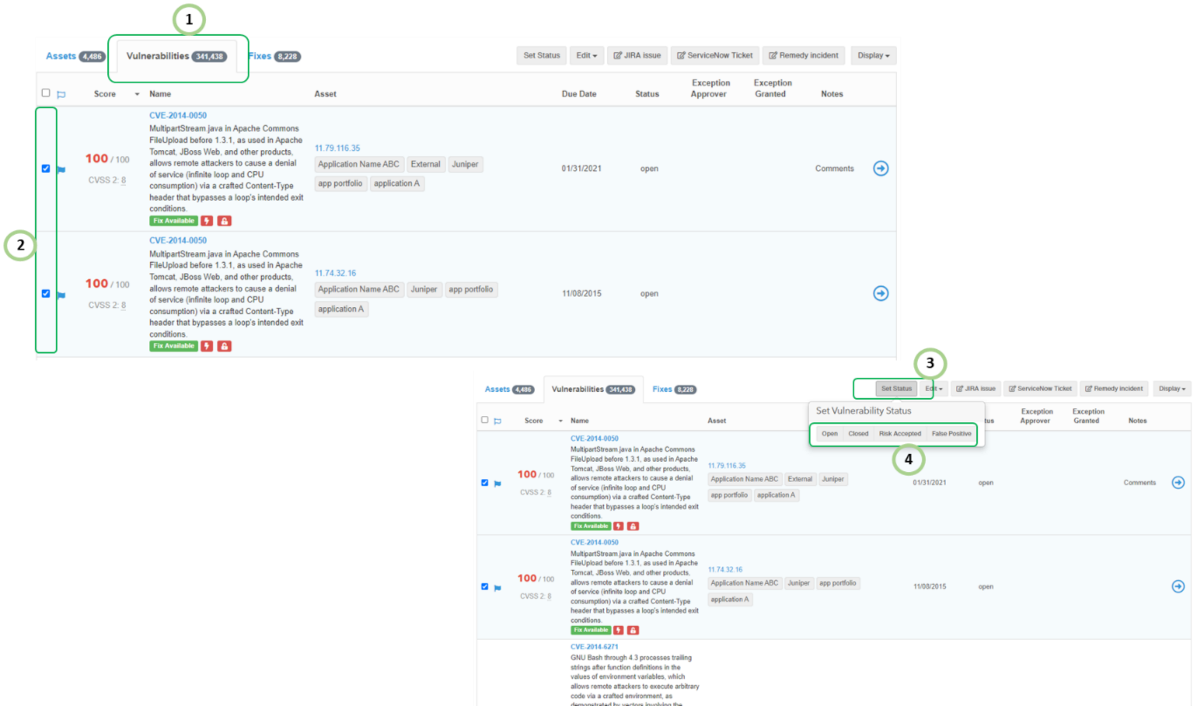
Closed: Closed vulnerabilities have been tracked as remediated by the Kenna platform. They no longer contribute in any way to the score of the asset. If Kenna rediscovers these vulnerabilities in new connector runs, they can be reopened. If status was manually set as ‘Closed’, then Kenna will no longer automatically manage the status of that vulnerability.

Risk Accepted: Kenna provides a ‘Risk Accepted’ status for those vulnerabilities which an organization has taken the decision not to fix. These vulnerabilities by do not affect the score of an asset and are not included in the default filters when creating Risk Meters. Note that they can be included by selecting the appropriate filter under ‘Vulnerability filters’ (discussed in the ‘Creating Risk Meters: Using Filters’ section).

False Positive: The last vulnerability status is a ‘False Positive’ status. This status is provided for scenarios where a finding is incorrectly detected by the originating scanner. Users can use this status to mark the vulnerability as such, and similar to a risk accepted status, removes it from asset score considerations and default Risk Meter creation filters.

Like asset statuses, vulnerability statuses can be modified as illustrated in the steps below and shown in the accompanying image.

1. Navigate to the Vulnerabilities view and select one or more vulnerabilities
2. Click on ‘Set Status’ and then modify the status of the vulnerability to the desired one.



☐	Score	Name	Asset	Due Date	Status	Exception Approver	Exception Granted	Notes
☑	100 / 100 CVSS 2: 8	CVE-2014-0050 MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions. Fix Available	11.79.116.35 Application Name ABC External Juniper app portfolio application A	01/31/2021	open			Comments
☑	100 / 100 CVSS 2: 8	CVE-2014-0050 MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions. Fix Available	11.74.32.16 Application Name ABC Juniper app portfolio application A	11/08/2015	open			
		CVE-2014-6271 GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the						

Note: The Kenna platform no longer updates the status of any vulnerability that has been manually changed to ‘False Positive’, ‘Risk Accepted’ or ‘Closed’.

Risk Meters / Asset Searches

An asset search is a logical grouping of assets. This is also called a Risk Meter, or a risk group. The grouping of assets can be done based on a number of ways in Kenna including any of the built-in filters on the right of the ‘VM Explore’ page, or using the custom query builder. Risk Meters are an important concept in Kenna as it can be the starting piece for a wide range of functionality, including the creation of dashboards. This is discussed in more depth in later sections of this document.

Asset Prioritization

The Asset Priority value in Kenna is used to incorporate risk appetite, for any individual asset, into the Kenna scoring methodology. The prioritization of an asset is a score between 1 and 10, with 10 being the default priority value of all assets. Asset priority of assets are used in calculation of the asset scores of assets (more of this in the ***scoring*** section) and they are directly proportional to the score of that asset. It can be considered a ‘weighting’ mechanism for calculating the score of an asset.

Scoring in Kenna – Vulnerability Score, Asset Score and Risk Score

There are 3 types of scoring within Kenna – vulnerability/risk score, asset score and Risk Meter scores.

- Risk score: Risk score or Kenna vulnerability score is the score assigned to each vulnerability within Kenna and varies from 0 to 100. Network vulnerabilities with a CVE ID are dynamically scored by Kenna based off machine learning, exploit and threat intel from more than 15 different feeds. For application vulnerabilities

(WASC-IDs, CWE-IDs and other unique IDs), the Kenna platform relies on the score brought in from the scanner. The score is normalized to 100.

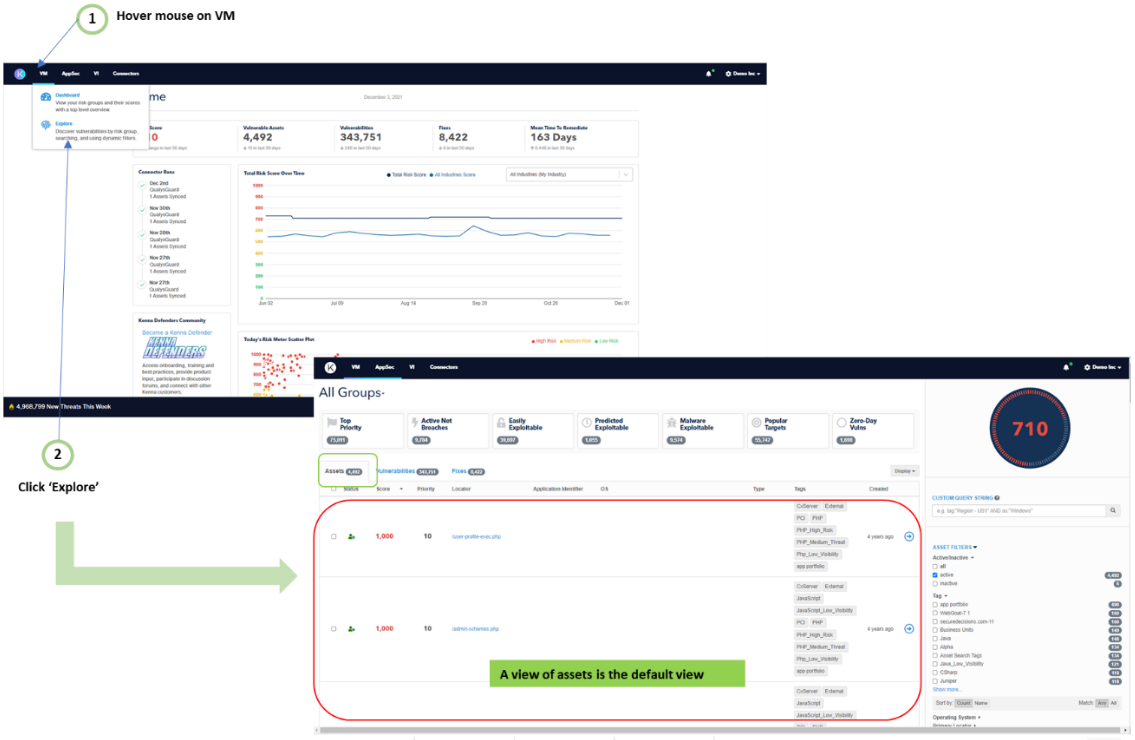
- Asset score: The score for an asset is the highest vulnerability score on that asset, multiplied by the priority of that asset. Asset scores can be 0 to 1,000. Closed and risk accepted vulnerabilities do not contribute to the Kenna asset score. Note that any assets that Kenna considers to be external because they lie out of the private IP space (10.*, 172.16.0.0 - 172.31.255.255 and 192.168.*) will have an additional 200 score bump. Assets without an IP address will also get a 200-score bump. Even with the score bump, the maximum possible score that an asset can have is 1,000.
- Risk Meter score: The Risk Meter score for a group of assets is the average of all non-zero assets that make up that Risk Meter.

Reference guides on Kenna help pages: https://help.kennasecurity.com/hc/en-us/articles/4402070116116-Understanding-Vulnerability-Asset-and-Risk-Meter-Scoring

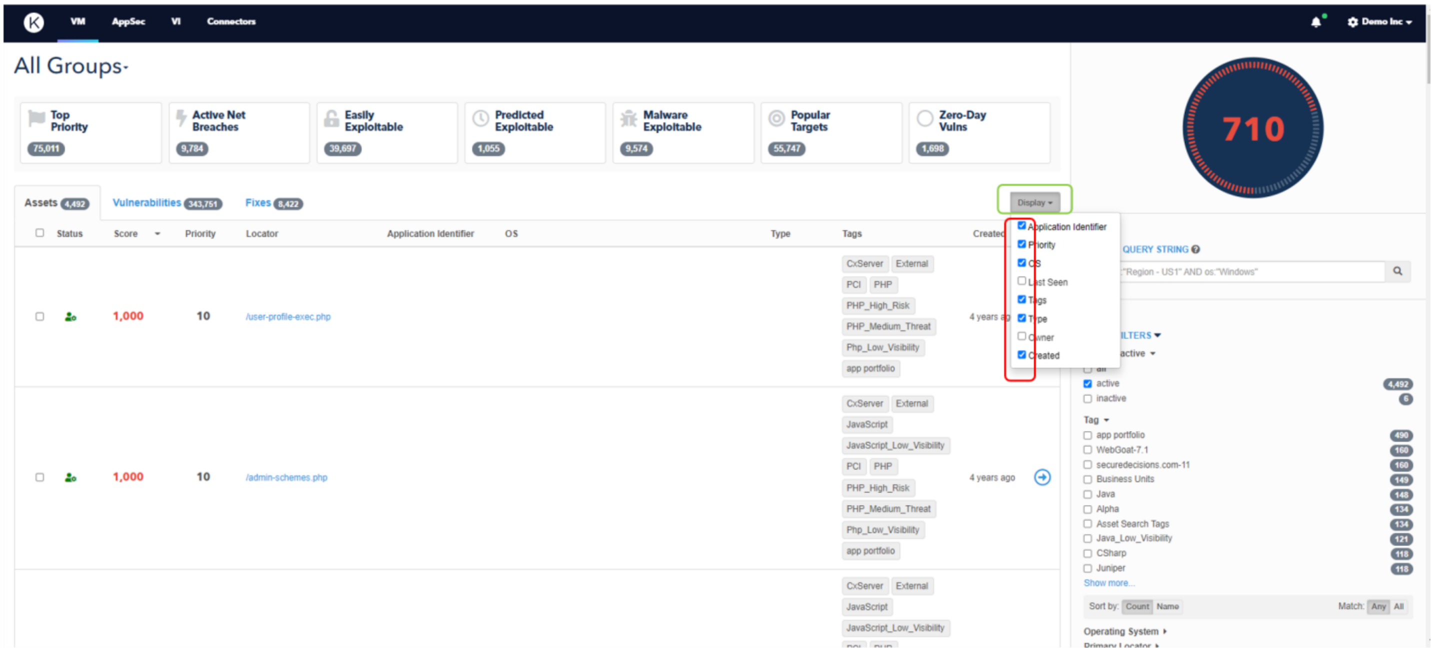
Common Operations within Kenna

Viewing Assets

Once logged into the Kenna platform, users can view all assets they have access to by navigating to the VM menu option and selecting 'Explore'. The default view is the Assets view as shown in the snippet.



Users can add or remove columns describing various attributes of the asset by selecting 'Display' and then checking or unchecking the desired attribute.



All Groups

Top Priority	Active Net Breaches	Easily Exploitable	Predicted Exploitable	Malware Exploitable	Popular Targets	Zero-Day Vulns
75,011	9,784	39,697	1,055	9,574	55,747	1,698

Assets 4,492 · Vulnerabilities 343,751 · Fixes 8,422

Display
- ☑ Application Identifier
- ☑ Priority
- ☑ OS
- ☐ Last Seen
- ☑ Tags
- ☑ Type
- ☐ Owner
- ☑ Created

☐	Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
☐		1,000	10	/user-profile-exec.php				CxServer, External PCI, PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ag
☐		1,000	10	/admin-schemes.php				CxServer, External JavaScript JavaScript_Low_Visibility PCI, PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
								CxServer, External JavaScript JavaScript_Low_Visibility	

QUERY STRING
"Region - US1" AND os:"Windows"

ILTERS
active
- ☐ all
- ☑ active 4,492
- ☐ inactive 6

Tag
- ☐ app portfolio 490
- ☐ WebGoat-7.1 160
- ☐ securedecisions.com-11 160
- ☐ Business Units 149
- ☐ Java 148
- ☐ Alpha 134
- ☐ Asset Search Tags 134
- ☐ Java_Low_Visibility 121
- ☐ CSharp 118
- ☐ Juniper 118

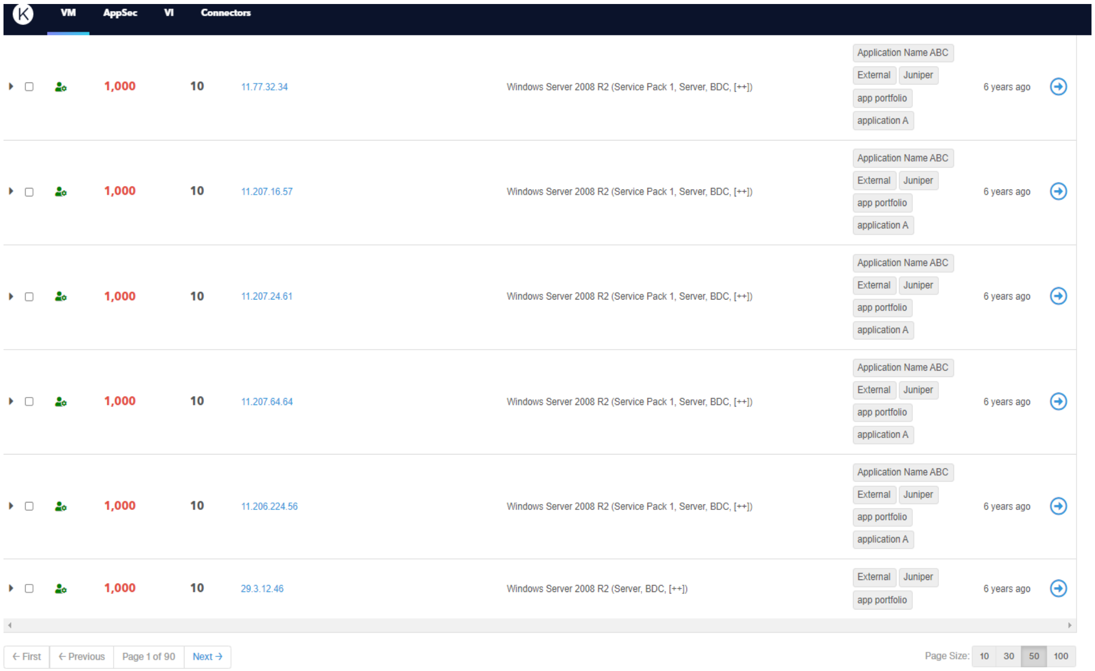
Show more...

Sort by: Count Name   Match: Any All

Operating System

Primary Locator

Users can increase the total number of assets that can be viewed on a page using the four (4) page options at the bottom right of the Assets page.

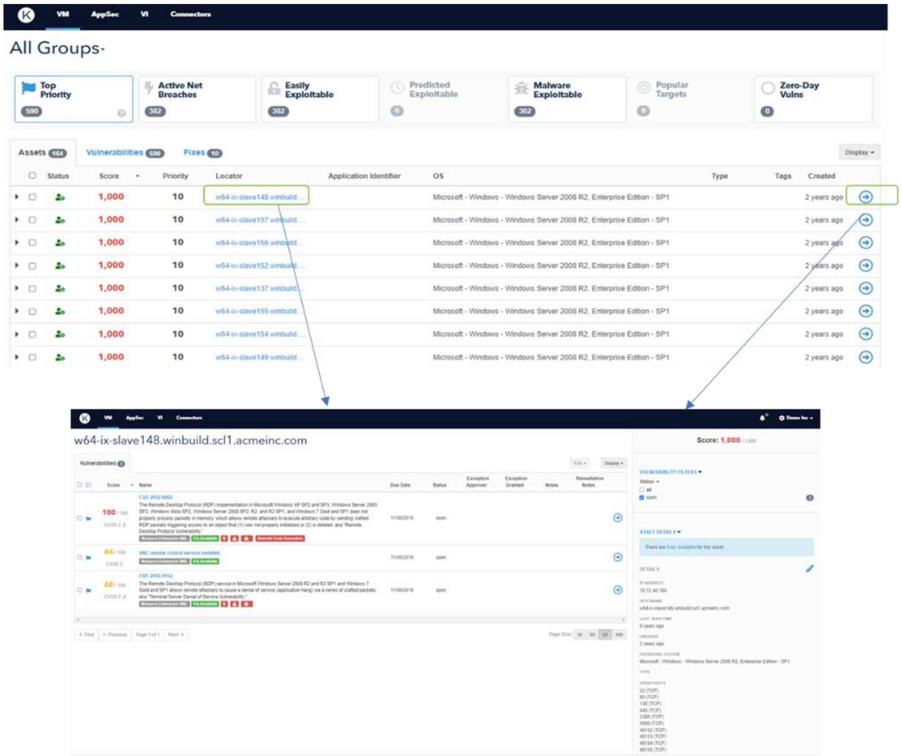


☐		1,000	10	11.77.32.34	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])	Application Name ABC External, Juniper app portfolio application A	6 years ago
☐		1,000	10	11.207.16.57	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])	Application Name ABC External, Juniper app portfolio application A	6 years ago
☐		1,000	10	11.207.24.61	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])	Application Name ABC External, Juniper app portfolio application A	6 years ago
☐		1,000	10	11.207.64.64	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])	Application Name ABC External, Juniper app portfolio application A	6 years ago
☐		1,000	10	11.206.224.56	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])	Application Name ABC External, Juniper app portfolio application A	6 years ago
☐		1,000	10	29.3.12.46	Windows Server 2008 R2 (Server, BDC, [++])	External, Juniper app portfolio	6 years ago

← First · ← Previous · Page 1 of 90 · Next →

Page Size: 10 30 50 100

To see details of a particular asset, click on the locator for that asset, or the blue arrow at the side right hand of every asset to go into the Asset Detail page.



All Groups-

Top Priority	Active Net Breaches	Easily Exploitable	Predicted Exploitable	Malware Exploitable	Popular Targets	Zero-Day Vulns
590	302	302	0	302	0	0

Assets 164 · Vulnerabilities 590 · Fixes 10

Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
	1,000	10	w64-ix-slave148.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave157.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave156.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave152.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave137.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave155.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave154.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago
	1,000	10	w64-ix-slave149.winbuild...		Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1			2 years ago

w64-ix-slave148.winbuild.scl1.acmeinc.com

Score: 1,000 / 1,000

Vulnerabilities 3

Score	Name	Due Date	Status	Exception Approver	Exception Granted	Notes	Remediation Notes
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability." Fix Available · Remote Code Execution	11/08/2019	open				
64 / 100 CVSS 2:	VNC remote control service installed Fix Available	11/08/2019	open				
60 / 100 CVSS 2: 4	CVE-2012-0152 The Remote Desktop Protocol (RDP) service in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (application hang) via a series of crafted packets, aka "Terminal Server Denial of Service Vulnerability." Fix Available	11/08/2019	open				

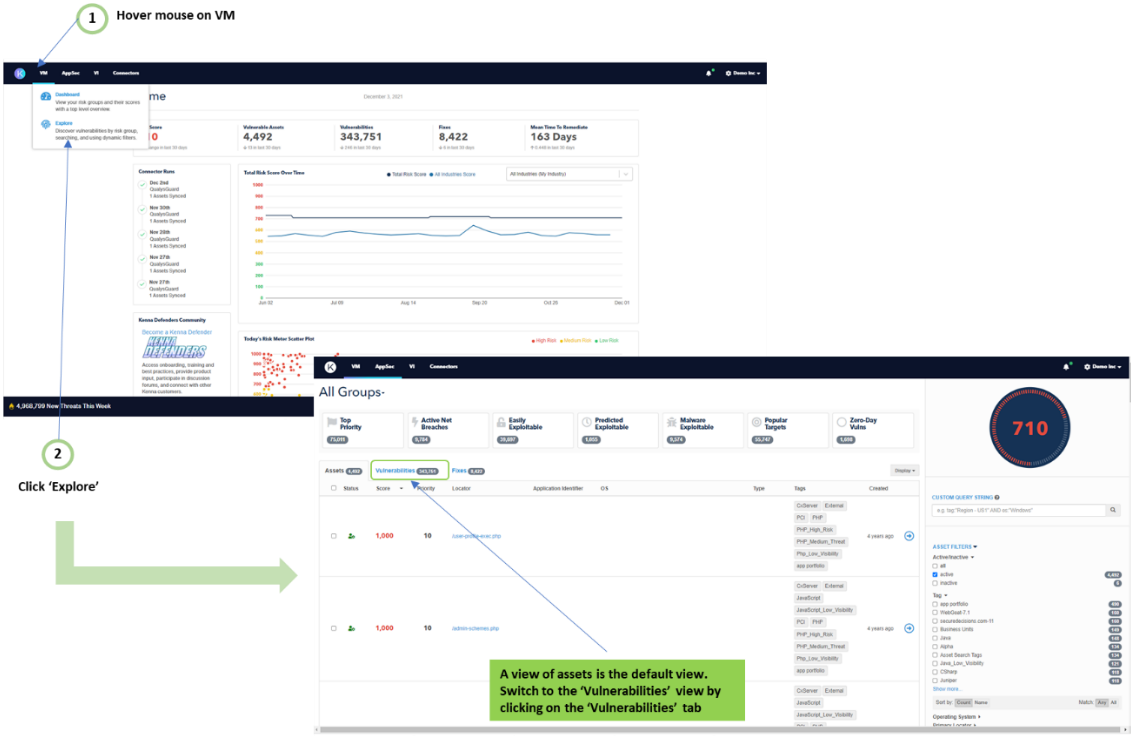
VULNERABILITY FILTERS
Status
□ all
☑ open

ASSET DETAILS
There are fixes available for this asset.

DETAILS
IP ADDRESS: 10.12.40.180
HOSTNAME: w64-ix-slave148.winbuild.scl1.acmeinc.com
LAST SEEN TIME: 8 years ago
CREATED: 2 years ago
OPERATING SYSTEM: Microsoft - Windows - Windows Server 2008 R2, Enterprise Edition - SP1
TYPE
OPEN PORTS: 22 (TCP), 80 (TCP), 135 (TCP), 445 (TCP), 3389 (TCP), 5900 (TCP), 49152 (TCP), 49153 (TCP), 49154 (TCP), 49155 (TCP)

Viewing Vulnerabilities

Once logged into the Kenna platform, navigating to the VM Explore page brings the user to the Assets view which is the default view on the Explore page. Once on the 'Explore' page, switch to the vulnerabilities view by clicking on 'Vulnerabilities' tab as shown below.

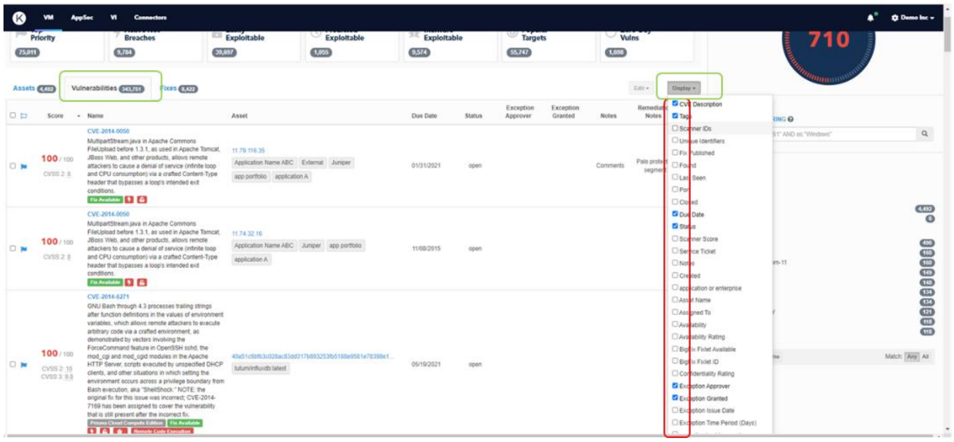

1 Hover mouse on VM

2 Click 'Explore'

A view of assets is the default view. Switch to the 'Vulnerabilities' view by clicking on the 'Vulnerabilities' tab

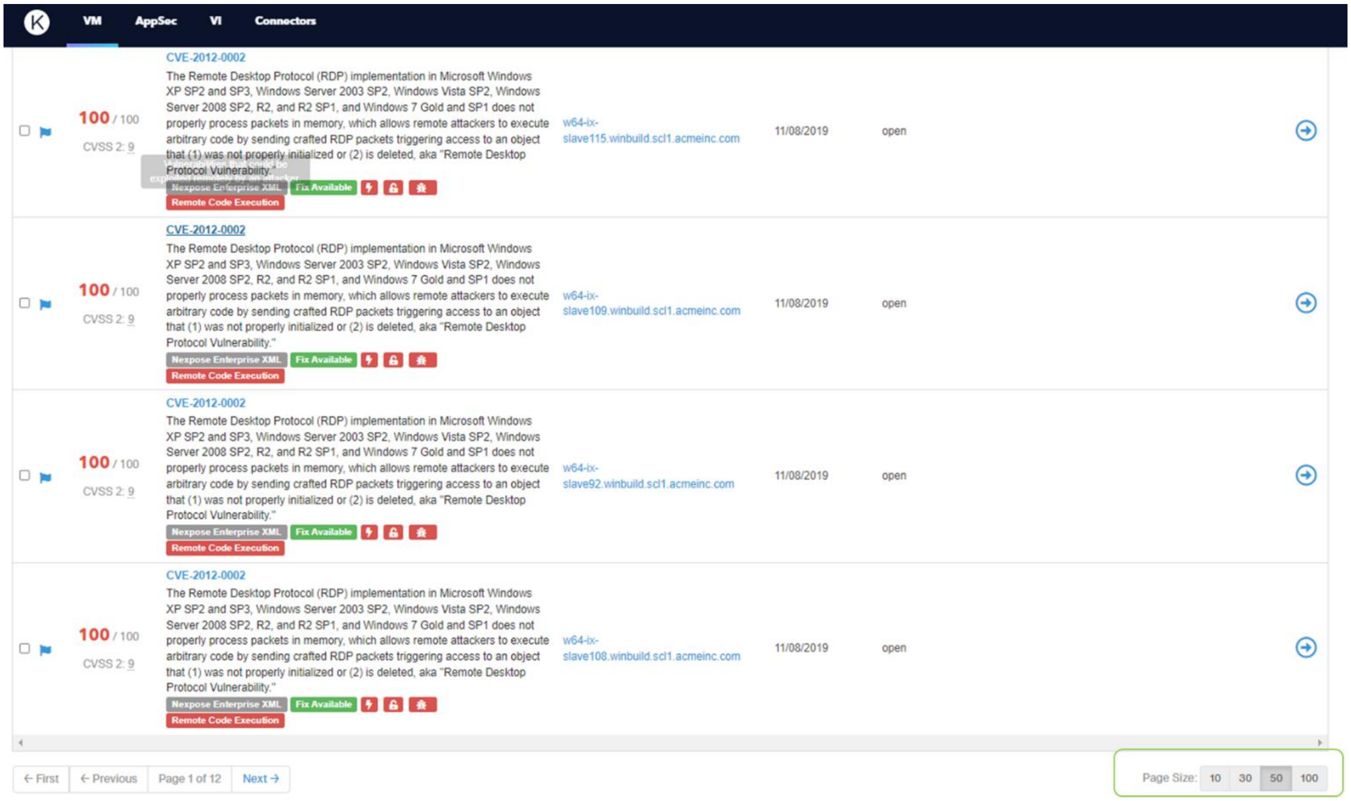
VM
AppSec
VI
Connectors
Dashboard
View your risk groups and their scores with a top level overview.
Explore
Discover vulnerabilities by risk group, searching, and using dynamic filters.
December 3, 2021
Vulnerable Assets 4,492
Vulnerabilities 343,751
Fixes 8,422
Mean Time To Remediate 163 Days
Connector Runs
Total Risk Score Over Time
Kenna Defenders Community
Become a Kenna Defender
Today's Risk Meter Scatter Plot
4,968,799 New Threats This Week
All Groups-
Top Priority 75,011
Active Net Breaches 9,784
Easily Exploitable 39,697
Predicted Exploitable 1,055
Malware Exploitable 9,574
Popular Targets 55,747
Zero-Day Vulns 1,698
Assets 4,492
Vulnerabilities 343,751
Fixes 8,422
710
CUSTOM QUERY STRING
ASSET FILTERS

Just like with Assets, users can show or hide columns fields of various attributes of the asset by selecting ‘Display’ and then checking or unchecking the desired attribute in the Vulnerabilities tab.



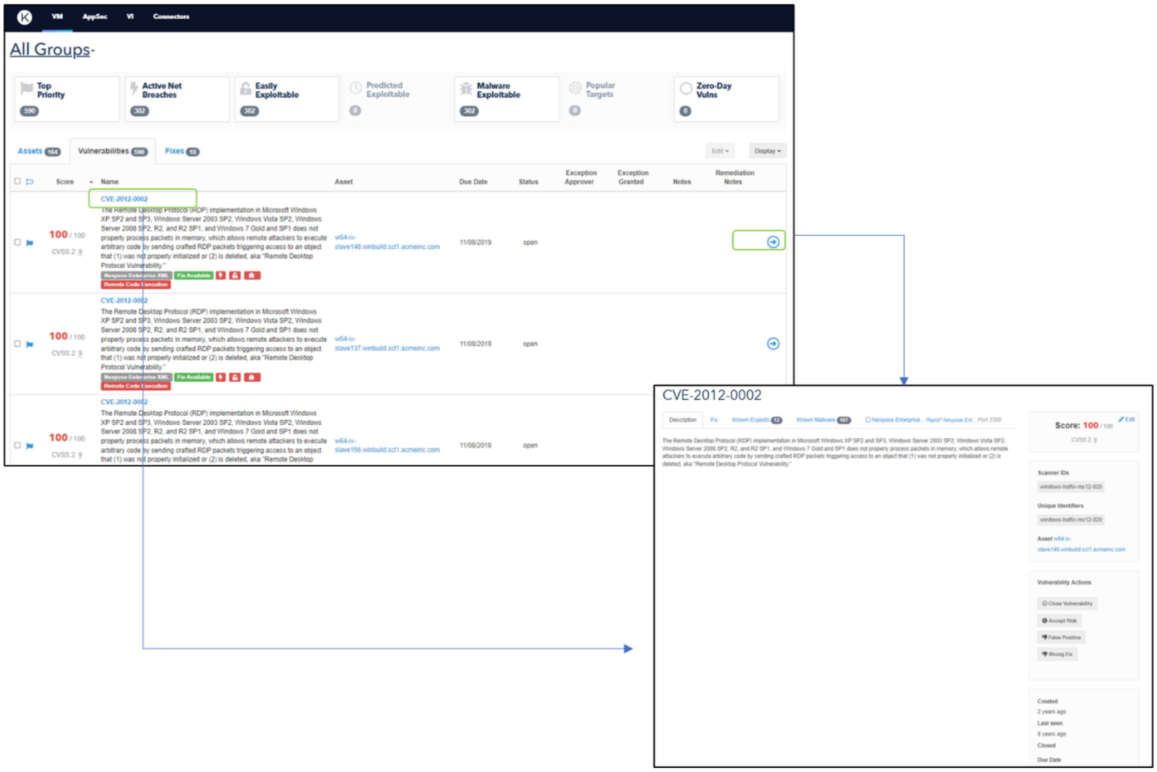
Score	Name	Asset	Due Date	Status	Exception Approver	Exception Granted	Notes	Remediation Notes
100 / 100 CVSS 2: 8	CVE-2014-0050 MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions.	11.79.116.35 Application Name ABC External Juniper app portfolio application A	01/31/2021	open			Comments	Palo prote segme
100 / 100 CVSS 2: 8	CVE-2014-0050 MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions.	11.74.32.16 Application Name ABC Juniper app portfolio application A	11/08/2015	open				
100 / 100 CVSS 2: 10 CVSS 3: 9.8	CVE-2014-6271 GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.	40a51c6bfb3c028ac83dd317b893253fb5188e9581e78398e1... tutum/influxdb:latest	05/19/2021	open				

Users can increase or decrease the total number of vulnerabilities shown on a page by selecting one of the pre-defined values at the bottom of the page.



100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."	w64-ix-slave115.winbuild.scl1.acmeinc.com	11/08/2019	open
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."	w64-ix-slave109.winbuild.scl1.acmeinc.com	11/08/2019	open
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."	w64-ix-slave92.winbuild.scl1.acmeinc.com	11/08/2019	open
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."	w64-ix-slave108.winbuild.scl1.acmeinc.com	11/08/2019	open

To see details of a particular vulnerability, click on the Name of that vulnerability, or on the blue arrow at the far side of the vulnerability in question, and you can see details of that vulnerability.



Score	Name	Asset	Due Date	Status	Exception Approver	Exception Granted	Notes	Remediation Notes
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability." Nexpose Enterprise XML · Fix Available · Remote Code Execution	w64-ix-slave148.winbuild.scl1.acmeinc.com	11/08/2019	open				
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability." Nexpose Enterprise XML · Fix Available · Remote Code Execution	w64-ix-slave137.winbuild.scl1.acmeinc.com	11/08/2019	open				
100 / 100 CVSS 2: 9	CVE-2012-0002 The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop	w64-ix-slave156.winbuild.scl1.acmeinc.com	11/08/2019	open				

CVE-2012-0002

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."

Score: 100 / 100
CVSS 2: 9

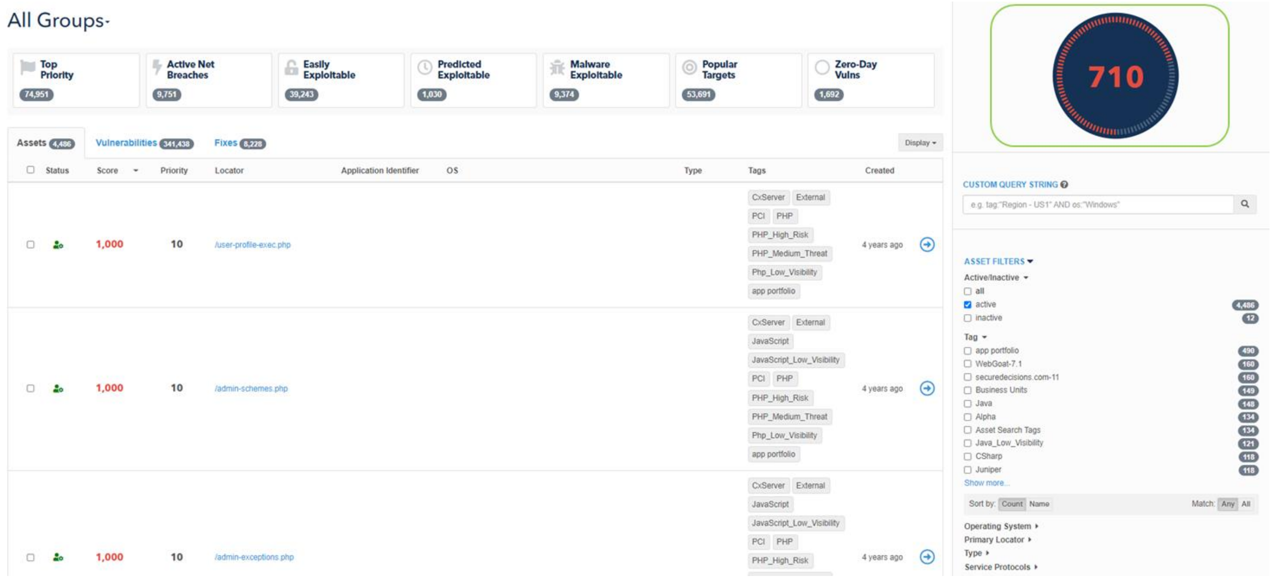
Scanner IDs: windows-hotfix-ms12-020
Unique Identifiers: windows-hotfix-ms12-020
Asset w64-ix-slave148.winbuild.scl1.acmeinc.com

Created: 2 years ago
Last seen: 8 years ago
Closed
Due Date

Viewing Risk Meters

Risk Meter on the Explore Page

Once logged into the Kenna platform, navigating to the VM Explore page brings the user to the Assets view which is the default view on the Explore page. At the upper right, the Risk Meter for the group of assets is shown. The default Risk Meter shown is for all assets that the user has access to.



Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
	1,000	10	/user-profile-exec.php				CxServer External PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
	1,000	10	/admin-schemes.php				CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
	1,000	10	/admin-exceptions.php				CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk	4 years ago

CUSTOM QUERY STRING

e.g. tag:"Region - US1" AND os:"Windows"

ASSET FILTERS

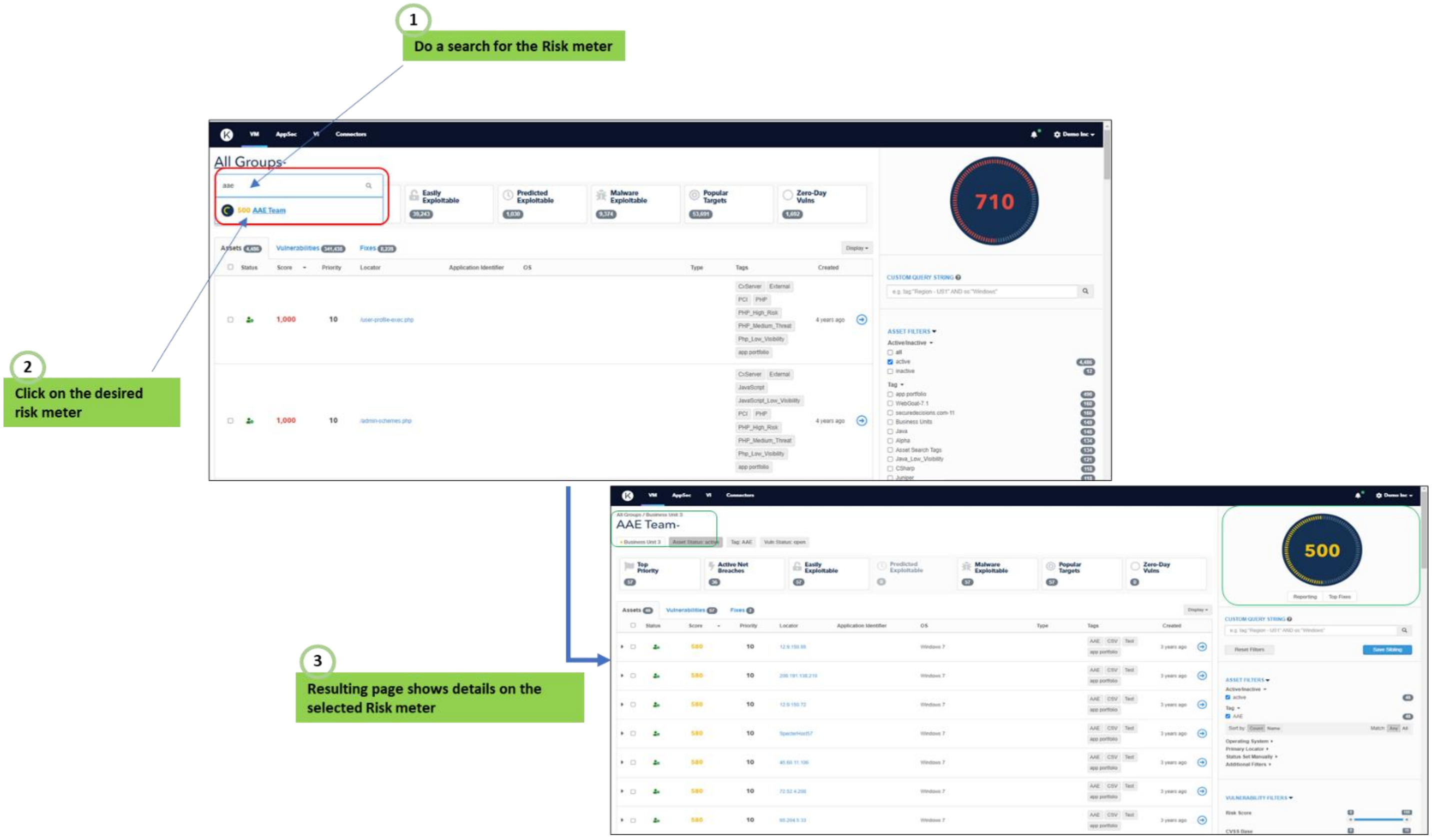
Active/Inactive
- ☐ all
- ☑ active 4,486
- ☐ inactive 12

Tag

Tag	Count
☐ app portfolio	490
☐ WebGoat-7.1	160
☐ securedecisions.com-11	160
☐ Business Units	149
☐ Java	148
☐ Alpha	134
☐ Asset Search Tags	134
☐ Java_Low_Visibility	121
☐ CSharp	118
☐ Juniper	118

Searching for a Risk Meter

A logged-on user can also search for a previously created Risk Meter. Close to the "All Groups'. Click on the arrowhead as captured in the image below and a search bar is seen. Search for the desired Risk Meter and select it from the returned results.



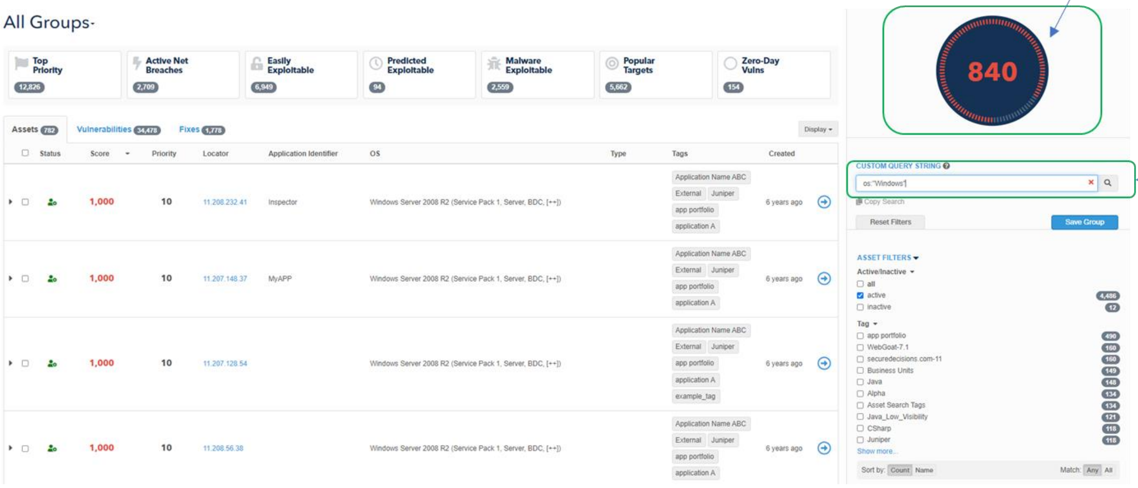
1 Do a search for the Risk meter

2 Click on the desired risk meter

3 Resulting page shows details on the selected Risk meter

Unsaved Risk Meters are also viewable in the same position. As captured in the 'Asset Searches' portion of this document, you can search for assets that meet a criterion and the Risk Meter for the returned group of assets is shown at the top of the page.

In the example below, a search for all Windows assets is done, and the resultant Risk Meter score is displayed.



All Groups-

Top Priority	Active Net Breaches	Easily Exploitable	Predicted Exploitable	Malware Exploitable	Popular Targets	Zero-Day Vulns
12,826	2,709	6,949	94	2,559	5,662	154

Assets 782 · Vulnerabilities 34,478 · Fixes 1,778 · Display

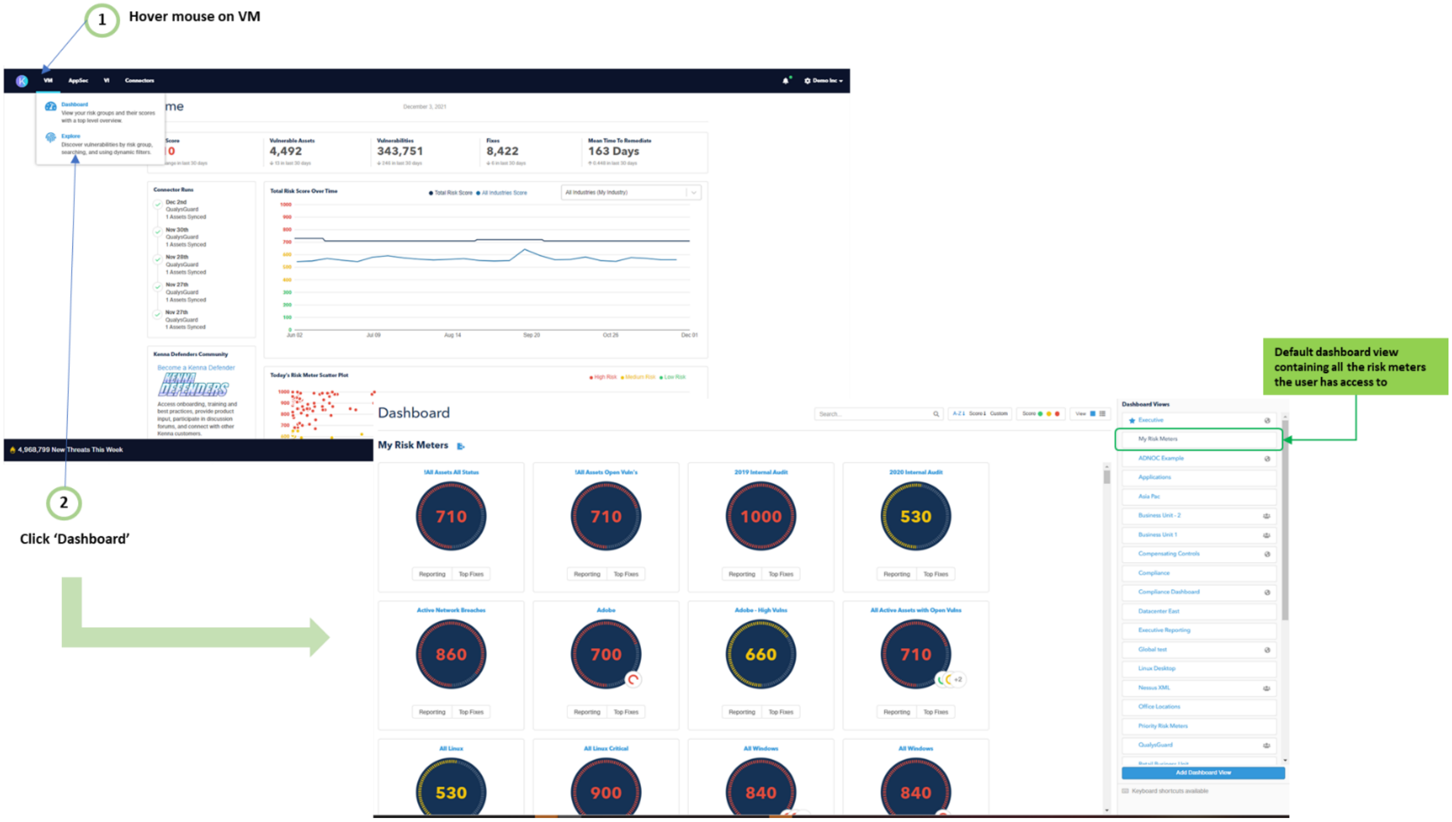
Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
	1,000	10	11.208.232.41	Inspector	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago
	1,000	10	11.207.148.37	MyAPP	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago
	1,000	10	11.207.128.54		Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A example_tag	6 years ago
	1,000	10	11.208.56.38		Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago

Unsaved risk meter – the outcome of adhoc asset searches

Unsaved risk meter – the outcome of adhoc asset searches

Risk Meter on the Dashboard Page

The dashboard menu is the area where the user can configure different collection of all, or a subset, of the Risk Meters that a user has access to. The default view in the dashboard is a user's 'My Risk Meters' dashboard view. This dashboard view shows all the Risk Meters that the logged-on user has access to.

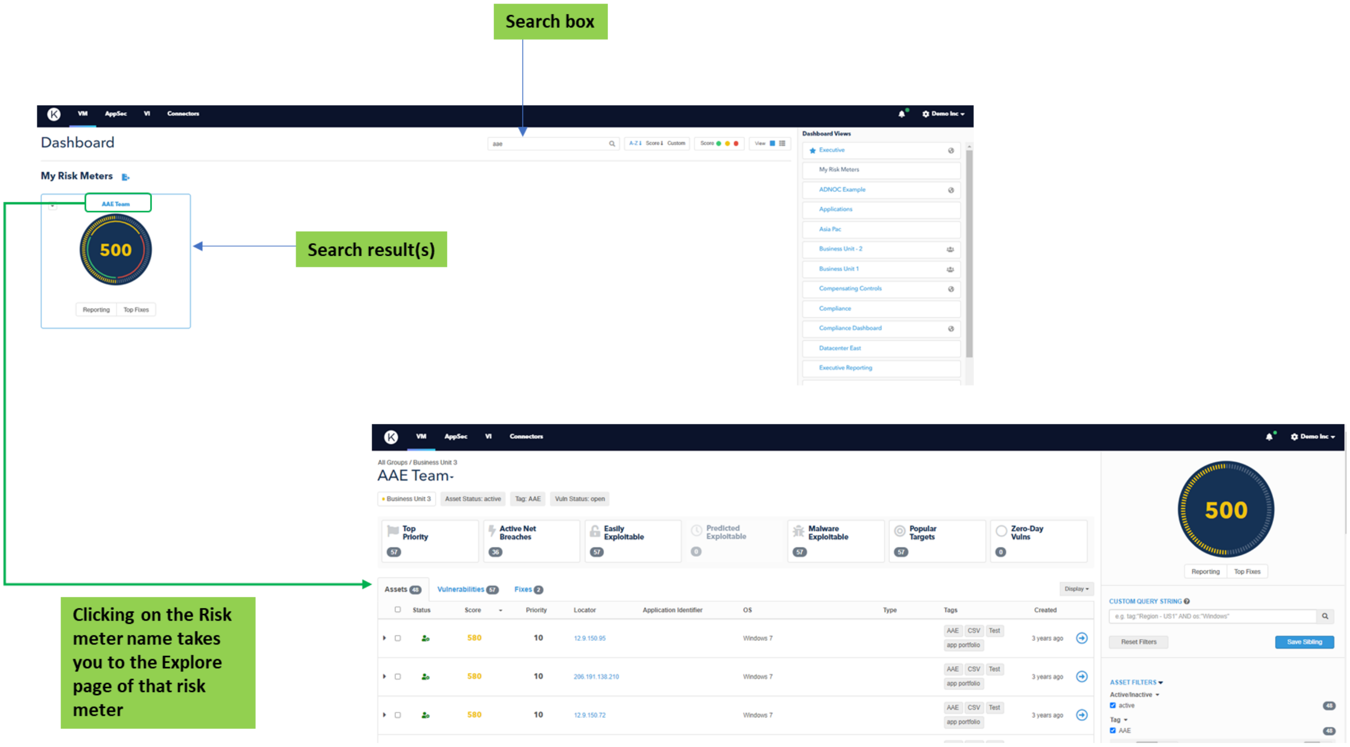


1 Hover mouse on VM

2 Click 'Dashboard'

Default dashboard view containing all the risk meters the user has access to

From this view, a user can search for additional Risk Meters as shown in the snippet below. When a particular Risk Meter is clicked, the user is taken to the VM Explore page for that particular Risk Meter.



Search box

Search result(s)

Clicking on the Risk meter name takes you to the Explore page of that risk meter

For additional operations that can be done on the dashboard view, please reference the help article here - https://help.kennasecurity.com/hc/en-us/articles/360036320311-Dashboard-Overview

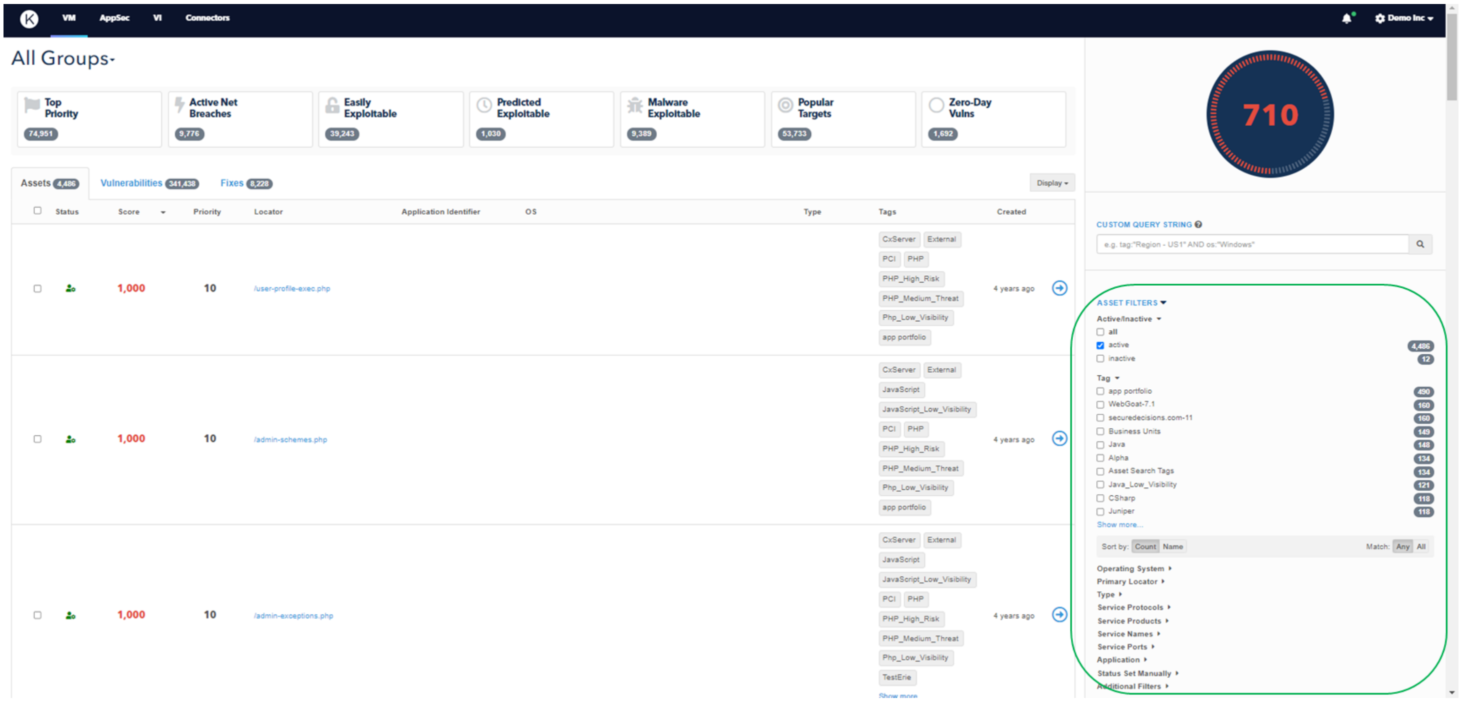
Deep Dive into Risk Meters / Asset Searches

As captured earlier, an asset search is a logical grouping of assets. They are also known as Risk Meters, or risk groups. The grouping of assets can be done based on a number of ways in Kenna including any of the built-in filters on the right of the 'VM Explore' page or using the custom query builder. Risk Meters are an important concept in Kenna as it can be the starting piece for a wide range of functionality, including the creation of dashboards.

Creating Risk Meters: Using Filters

Asset searches can be created using any of the filters located at the right hand of the VM Explore page. Once a filter, or a combination of filters, is selected, the assets that meet the condition for that filter are returned. The filters shown are largely divided into Asset and Vulnerability filters.

Asset filters: Some of the common filters include Asset status (active/inactive/all), Asset Tags, Operating System, Primary locators. A snippet of the asset filters is shown below.



All Groups

Top Priority	Active Net Breaches	Easily Exploitable	Predicted Exploitable	Malware Exploitable	Popular Targets	Zero-Day Vulns
74,951	9,776	39,243	1,030	9,389	53,733	1,692

Assets 4,486 Vulnerabilities 341,438 Fixes 8,228

☐	Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
☐		1,000	10	/user-profile-exec.php				CxServer External PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☐		1,000	10	/admin-schemes.php				CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☐		1,000	10	/admin-exceptions.php				CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility TestErie Show more	4 years ago

CUSTOM QUERY STRING

e.g. tag:"Region - US1" AND os:"Windows"

ASSET FILTERS

Active/Inactive

☐ all	
☑ active	4,486
☐ inactive	12

Tag

☐ app portfolio	490
☐ WebGoat-7.1	160
☐ securedecisions.com-11	160
☐ Business Units	149
☐ Java	148
☐ Alpha	134
☐ Asset Search Tags	134
☐ Java_Low_Visibility	121
☐ CSharp	118
☐ Juniper	118

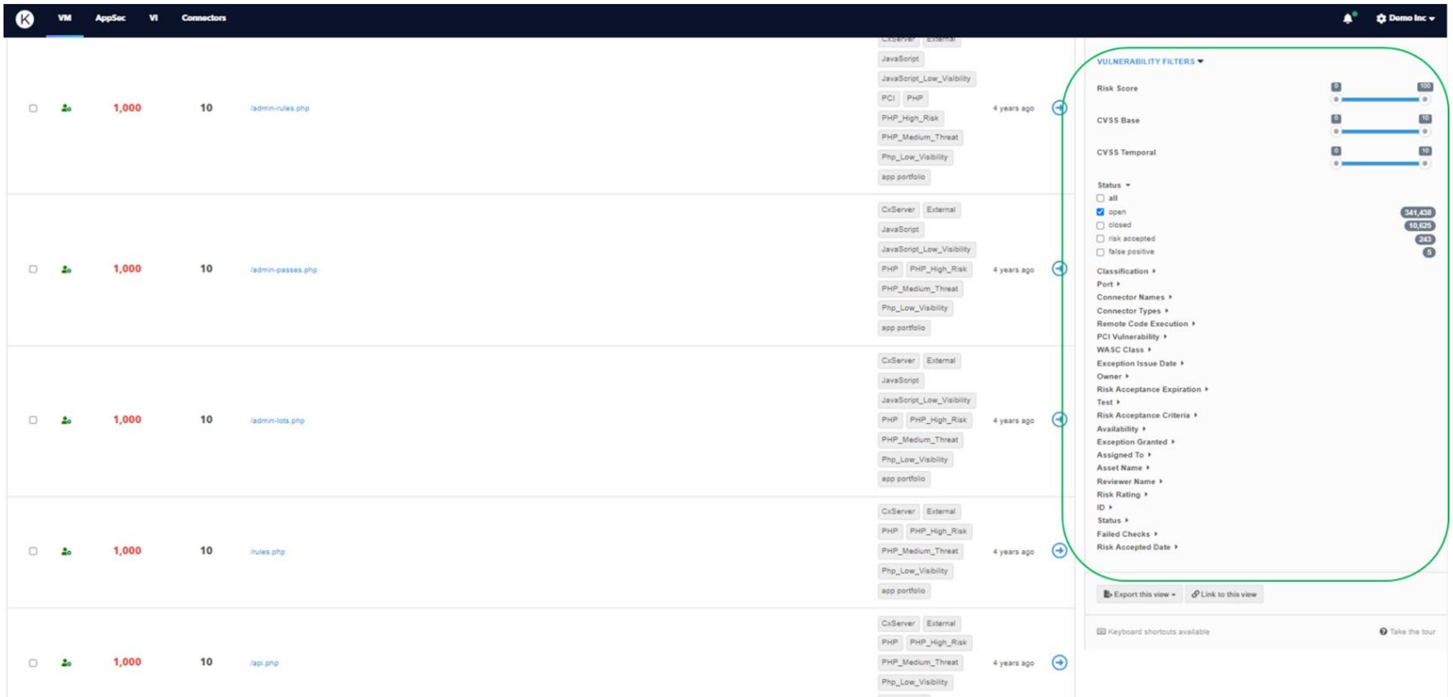
Show more...

Sort by: Count Name Match: Any All

Operating System
Primary Locator
Type
Service Protocols
Service Products
Service Names
Service Ports
Application
Status Set Manually
Additional Filters

Vulnerability filters: Some of the common filters include the following: Risk score (a slider), Vulnerability Status (all/open/closed/risk accepted/false positive), Connector Types, Connector Names. Any custom fields that have been created with the 'faceted search' option will also be shown as a filter under the vulnerability filters.

A snippet of the vulnerability filters is shown in the next image.



☐	Status	Score	Priority	Locator	Tags	Created
☐		1,000	10	/admin-rules.php	CxServer External JavaScript JavaScript_Low_Visibility PCI PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☐		1,000	10	/admin-passes.php	CxServer External JavaScript JavaScript_Low_Visibility PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☐		1,000	10	/admin-lots.php	CxServer External JavaScript JavaScript_Low_Visibility PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☐		1,000	10	/rules.php	CxServer External PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility app portfolio	4 years ago
☐		1,000	10	/api.php	CxServer External PHP PHP_High_Risk PHP_Medium_Threat Php_Low_Visibility	4 years ago

VULNERABILITY FILTERS

Risk Score 0 100
CVSS Base 0 10
CVSS Temporal 0 10

Status

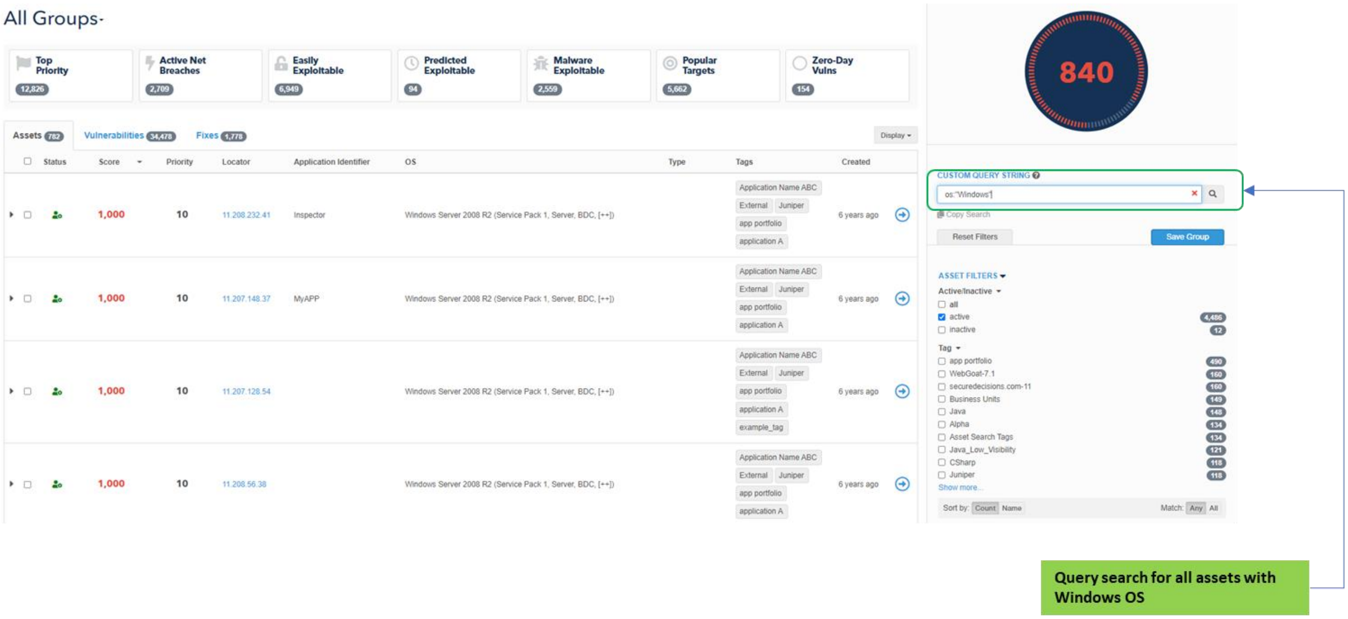
☐ all	
☑ open	341,438
☐ closed	10,625
☐ risk accepted	243
☐ false positive	5

Classification
Port
Connector Names
Connector Types
Remote Code Execution
PCI Vulnerability
WASC Class
Exception Issue Date
Owner
Risk Acceptance Expiration
Test
Risk Acceptance Criteria
Availability
Exception Granted
Assigned To
Asset Name
Reviewer Name
Risk Rating
ID
Status
Failed Checks
Risk Accepted Date

Creating Risk Meters: Using Custom Queries

A flexible way for creating asset searches is using the custom query. An example of such a query is a search of all assets that are running the Windows OS using the query:

os: “Windows”



All Groups

Top Priority	Active Net Breaches	Easily Exploitable	Predicted Exploitable	Malware Exploitable	Popular Targets	Zero-Day Vulns
12,826	2,709	6,949	94	2,559	5,662	154

Assets 782 · Vulnerabilities 34,478 · Fixes 1,778

Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
	1,000	10	11.208.232.41	Inspector	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago
	1,000	10	11.207.148.37	MyAPP	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago
	1,000	10	11.207.128.54		Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A example_tag	6 years ago
	1,000	10	11.208.56.38		Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago

840

CUSTOM QUERY STRING: os:"Windows"

ASSET FILTERS

Active/Inactive

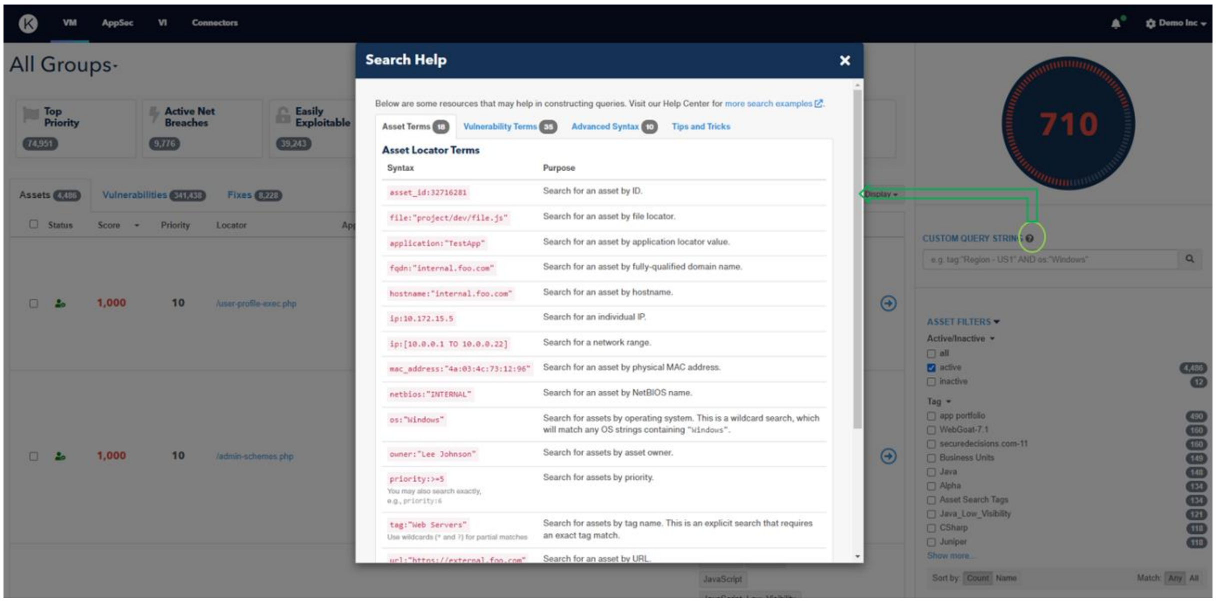
□ all	
☑ active	4,486
□ inactive	12

Tag

□ app portfolio	490
□ WebGoat-7.1	160
□ securedecisions.com-11	160
□ Business Units	149
□ Java	148
□ Alpha	134
□ Asset Search Tags	134
□ Java_Low_Visibility	121
□ CSharp	118
□ Juniper	118

Query search for all assets with Windows OS

For examples of the type of queries that can be done, click on the help sign as shown in the image below.



Search Help

Below are some resources that may help in constructing queries. Visit our Help Center for more search examples.

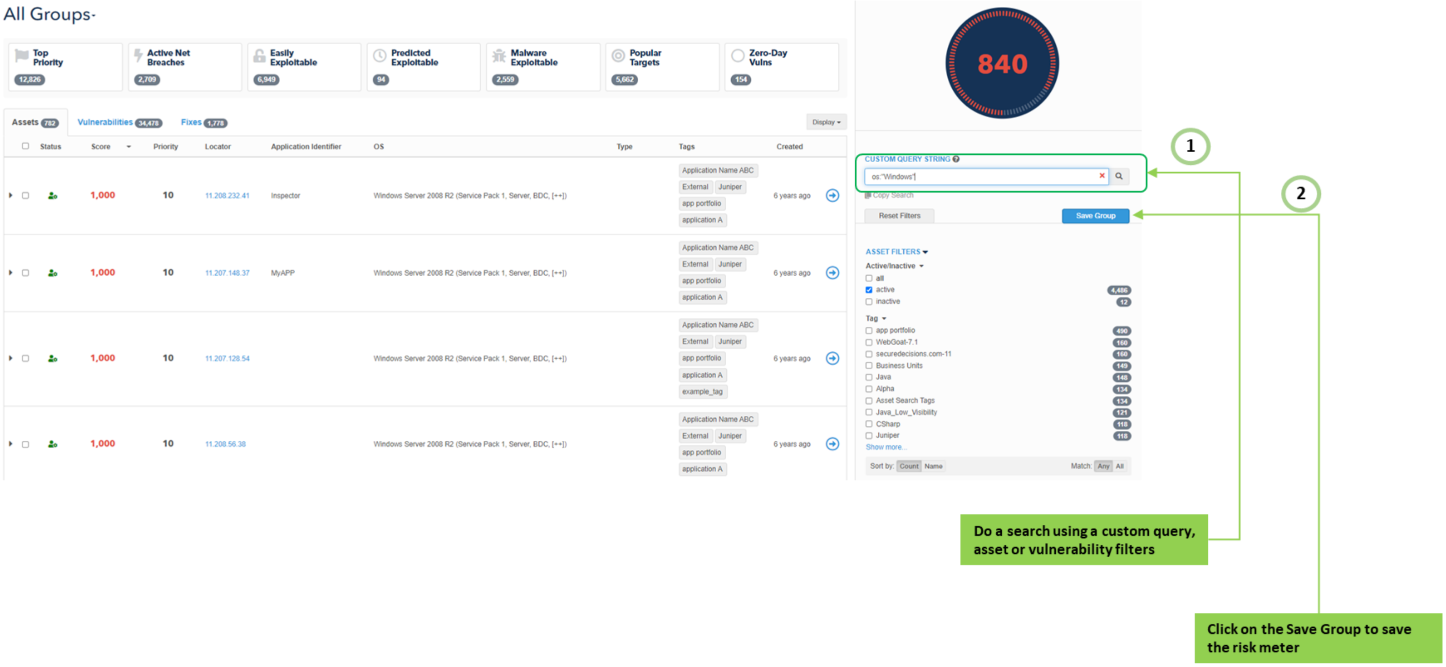
Asset Terms 18 · Vulnerability Terms 35 · Advanced Syntax 10 · Tips and Tricks

Asset Locator Terms

Syntax	Purpose
`asset_id:32716281`	Search for an asset by ID.
`file:"project/dev/file.js"`	Search for an asset by file locator.
`application:"TestApp"`	Search for an asset by application locator value.
`fqdn:"internal.foo.com"`	Search for an asset by fully-qualified domain name.
`hostname:"internal.foo.com"`	Search for an asset by hostname.
`ip:10.172.15.5`	Search for an individual IP.
`ip:[10.0.0.1 TO 10.0.0.22]`	Search for a network range.
`mac_address:"4a:03:4c:73:12:96"`	Search for an asset by physical MAC address.
`netbios:"INTERNAL"`	Search for an asset by NetBIOS name.
`os:"Windows"`	Search for assets by operating system. This is a wildcard search, which will match any OS strings containing "Windows".
`owner:"Lee Johnson"`	Search for assets by asset owner.
`priority:>=5` You may also search exactly, e.g., `priority:6`	Search for assets by priority.
`tag:"Web Servers"` Use wildcards (* and ?) for partial matches	Search for assets by tag name. This is an explicit search that requires an exact tag match.
`url:"https://external.foo.com"`	Search for an asset by URL.

Saving Risk Meters

Once an asset search has been done, the results can be saved.



□	Status	Score	Priority	Locator	Application Identifier	OS	Type	Tags	Created
□		1,000	10	11.208.232.41	Inspector	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago
□		1,000	10	11.207.148.37	MyAPP	Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago
□		1,000	10	11.207.128.54		Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A example_tag	6 years ago
□		1,000	10	11.208.56.38		Windows Server 2008 R2 (Service Pack 1, Server, BDC, [++])		Application Name ABC External Juniper app portfolio application A	6 years ago

CUSTOM QUERY STRING: os:"Windows"

ASSET FILTERS

Active/Inactive

□ all	
☑ active	4,486
□ inactive	12

Tag

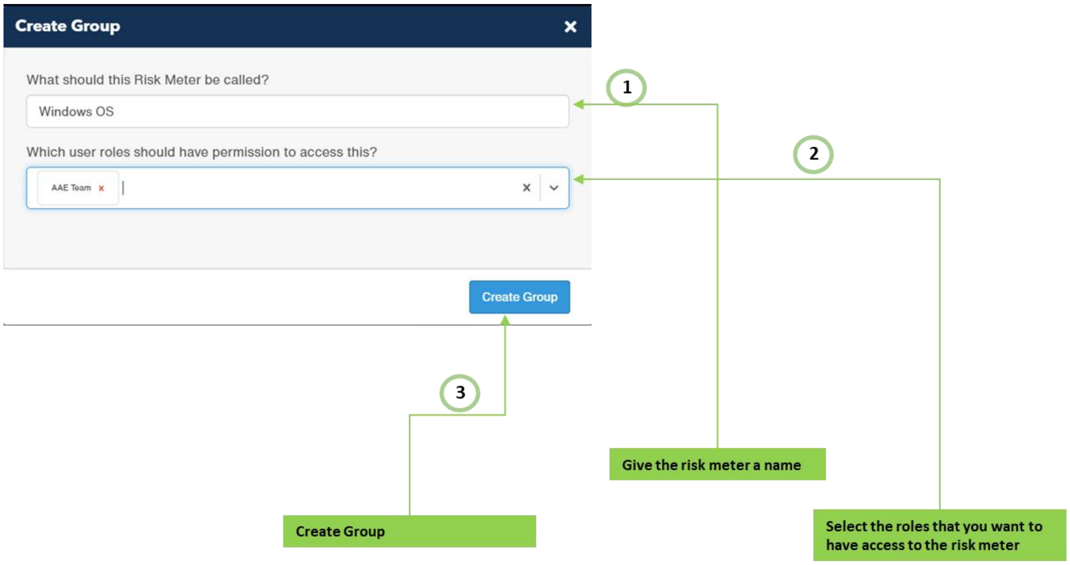
□ app portfolio	490
□ WebGoat-7.1	160
□ securedecisions.com-11	160
□ Business Units	149
□ Java	148
□ Alpha	134
□ Asset Search Tags	134
□ Java_Low_Visibility	121
□ CSharp	118
□ Juniper	118

Show more...

Sort by: Count Name   Match: Any All

Do a search using a custom query, asset or vulnerability filters

Click on the Save Group to save the risk meter



What should this Risk Meter be called?: Windows OS

Which user roles should have permission to access this?: AAE Team

Give the risk meter a name

Select the roles that you want to have access to the risk meter

Create Group

Some of the advantages of saving a Risk Meter:

1. Reporting is done on every saved Risk Meter. The various metrics for a Risk Meter are calculated and stored from the creation date of that Risk Meter. This is one of the more important functionalities of a Risk Meter and will be reviewed in a bit more detail in the next section.
2. Risk Meters can be added to a dashboard for focused attention.
3. Risk Meters are used to regulate the assets a particular role can access on the Kenna platform.

4. Risk Meters are automatically updated with new assets that meet the condition for that search.
5. Time savings from having to do the Risk Meter search every time.

Hierarchical Risk Meters (HRM)

HRMs are a relatively new feature within Kenna.VM which allows large enterprises to simplify asset management by organizing Risk Meters more intuitively. Child Risk Meters can now be added to Risk Meters, where the child is a subset of its parent with additive filters, enabling a better visual hierarchy and a more intuitive way to assign permissions. The assets and vulnerabilities included in any descendent group are determined by that group's immediate filter criteria, as well as all the filter criteria for any ancestors above it in the hierarchy.

Due to more restrictive criteria being added the further down the hierarchy you go, a child group will always show fewer (or at most, the same) assets and vulnerabilities than its parent group.

A few things to note with HRMs:

- All descendant Risk Meters inherit user role permissions from their parent. For example, if you have access to a parent Risk Meter, you will have access to all its descendants.
- Editing a parent impacts all descendant Risk Meters.
- Deleting a parent removes all descendant Risk Meters.
- Each descendant Risk Meter (parent, child, grandchild etc.) has its own independent Reporting and Top Fixes views.
- Each descendant Risk Meter has its own score.
- You can create up to 10 nested levels of descendant groups from the root parent Risk Meter.
- There is no limit to how many children a Risk Meter can have. Only hierarchy depth is limited, not breadth.

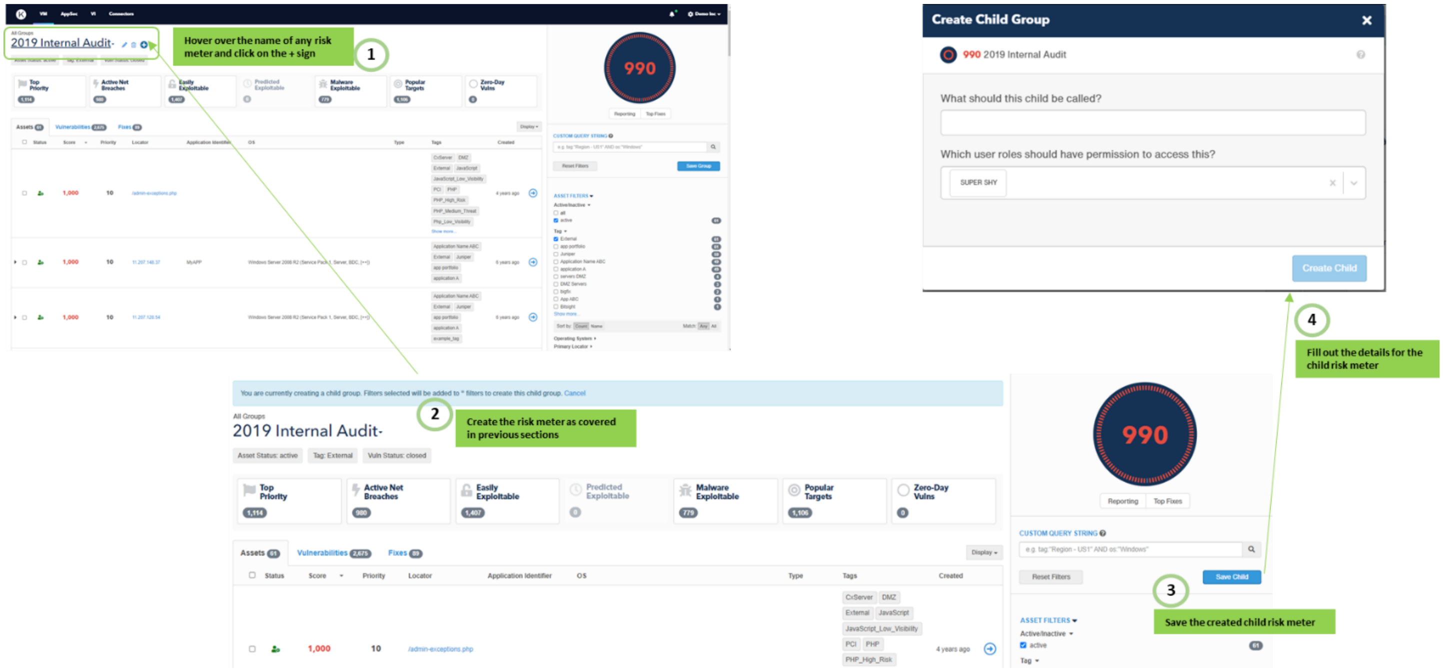
Creating HRMs

Note that the HRM functionality is not enabled by default and so if not enabled on an organization's platform, please have the administrators open a support ticket for this feature to be turned ON.

To create a HRM from the UI, carry out the following steps.

1. Navigate to the Risk Meter which is to be the parent.
2. Hover over the Risk Meter name. Additional icons are shown; click on the plus (+) icon.
3. Make modifications to the query and/or filters to obtain the desired asset grouping.
4. Click on the 'Save Child' button.
5. Fill out the details of the child Risk Meter.

Screenshots of this process are provided below.



1 Hover over the name of any risk meter and click on the + sign

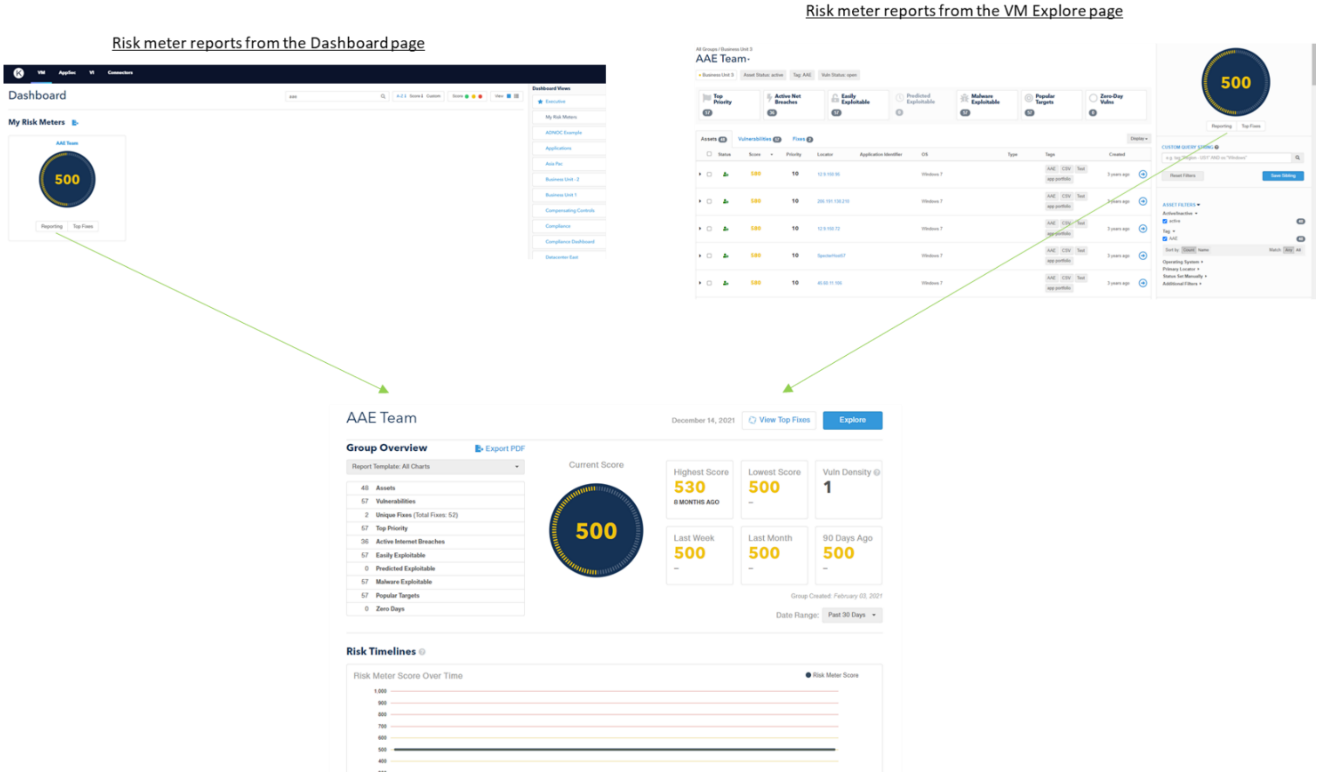
2 Create the risk meter as covered in previous sections

3 Save the created child risk meter

4 Fill out the details for the child risk meter

Uses of Risk Meters: Risk Meter Reports – Metrics and Trend Data

Risk Meter reports visualize your trending risk over time. As soon as a Risk Meter or Asset Group is created in Kenna, nightly captures of data begin to create the metric displayed in the report. You can access reports by clicking on the 'Reporting' icon in the bottom left corner of any Risk Meter on the Dashboard, or a Saved Risk Meter on the Explore page.


Risk meter reports from the Dashboard page

Risk meter reports from the VM Explore page

All items in the reports are updated during nightly jobs, except for the following items which present live data: Mean Time to Remediate, New Vulnerabilities Found, and Total Closed Vulnerabilities.

Note: If you edit the search query for a Risk Meter, you may see changes in asset and vulnerability counts in our reports. Also, if you delete a Risk Meter, you will delete all historical data previously collected for that meter.

Some reports that you get from the Risk Meter reporting page include:

Risk Timelines

- Trending Graph – Total Assets and Vulnerabilities Over Time
- Trending Graph – Active Assets and Open Vulnerabilities Over Time

Current Risk Information

- Open Vulnerabilities by Risk Level
- Open Vulnerabilities by Asset Tag
- Open Vulnerabilities by Operating System
- Open Vulnerabilities by Score
- Active Assets by Risk Level

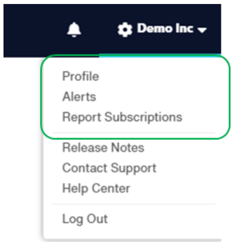
Many more such reports are available. Please review a sample report to see all the information that is available to you. For more information, kindly visit this Kenna help article – https://help.kennasecurity.com/hc/en-us/articles/202010278-Risk-Meter-Reporting

Settings Page

To view the settings page, click on the Gear icon (item 6 in Figure 1.1 and Figure 1.2). The menus that will be visible will depend on if the user is an administrative or a non-administrative user on the Kenna platform.

Non-Admin Users

The following options are available on the Settings menu for non-administrative users



Profile: The user is able to setup basic settings in their profile. The following items can be viewed/modified:

- First Name
- Last Name
- Email
- Phone

A user is also able to make password changes. The set password is not viewable, and the user must know the current password to be able to make any changes. Note that email addresses are expected to be unique within a shared Kenna environment.

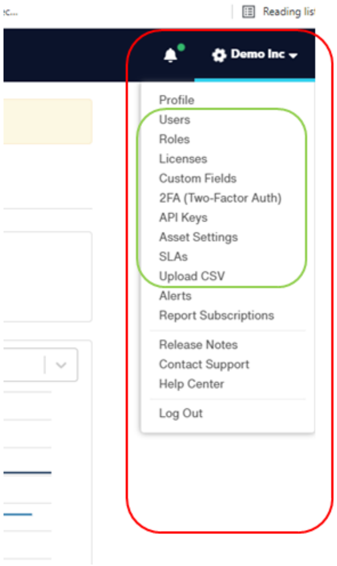
Alerts. Different alerts can be setup in the Settings → Alerts menu option. Alerts can be set for items like changes in Risk Meter risk level changes, identification of new internet breaches, and many more types of alerts. Both email and in-app alerts can be setup for each alert type. Please see this page for all possible alerts that can be set up - https://help.kennasecurity.com/hc/en-us/articles/211348246-How-do-I-set-up-Alerting-.

Report Subscriptions: The Kenna Security platform provides the ability to create and maintain any number of scheduled email alerts that will invite the recipient to view specific configured Risk Meter reports. The report subscriptions page can be accessed in the Settings → Report Subscriptions icon. User can request for reports for one or more Risk Meters on a Daily, Weekly, or Monthly schedule.

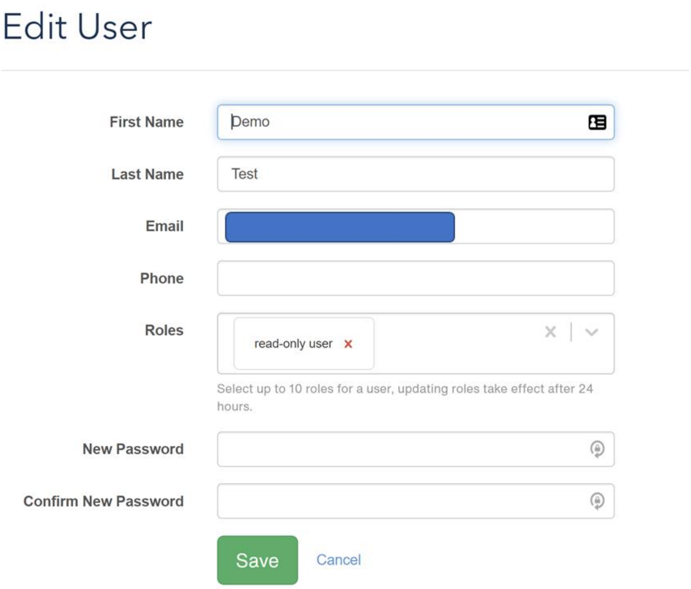
The user receives a link to log into Kenna, view the reports within the UI and if desired, export them to PDF.

Administrative Users

In addition to the 3 options available in the non-administrative described above, the following options are available on the Settings menu for administrative users:



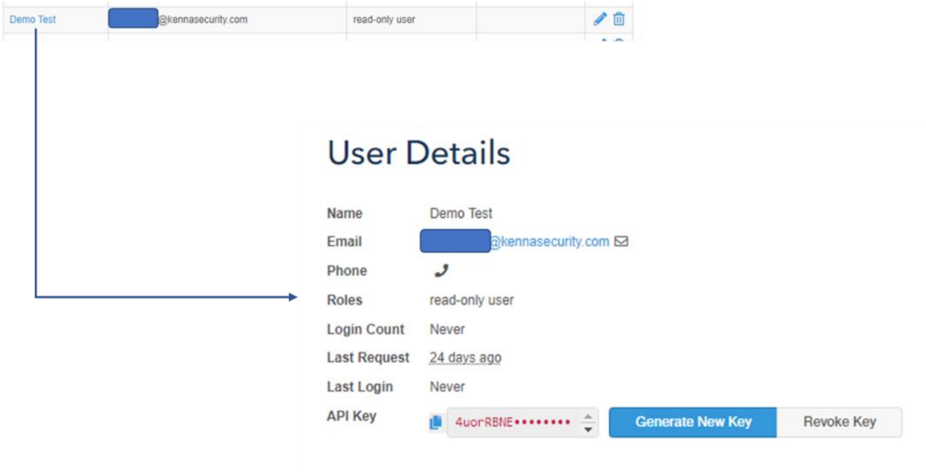
Users: This page is used by administrators to create, update, and manage users on their Kenna platform. This view allows for the modification of user attributes like first and last name, email, phone number, and user roles.



Edit User

First Name	Demo
Last Name	Test
Email	[redacted]
Phone	
Roles	read-only user ×
	Select up to 10 roles for a user, updating roles take effect after 24 hours.
New Password	
Confirm New Password	

A less-used functionality of the user menu is the ability to manage a single user's API access by generating a new key or revoking existing an API key for that user. Simply click on the username to reveal the 'User Details' page, and then generate or revoke an API key.

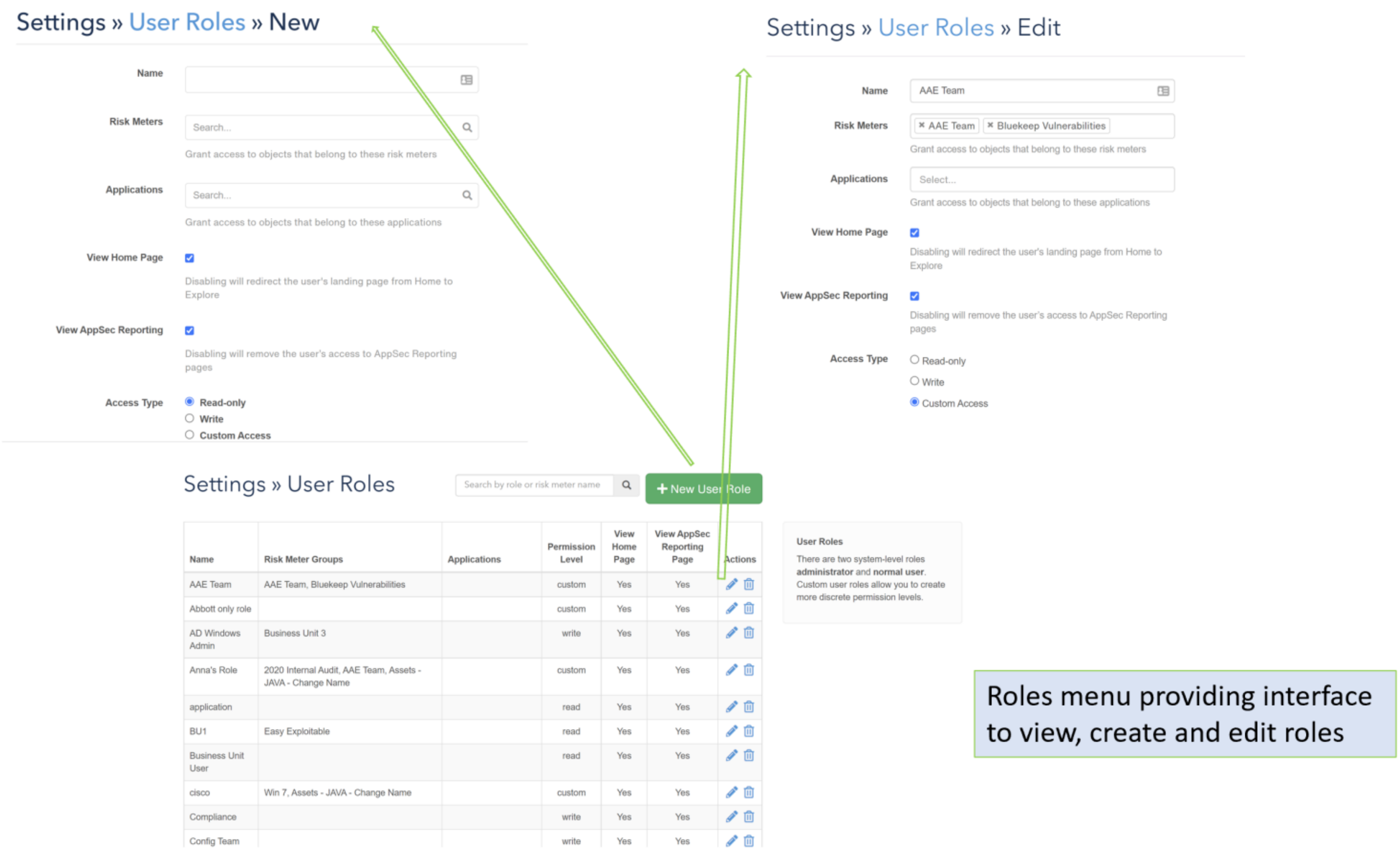


Demo Test	[redacted]@kennasecurity.com	read-only user

User Details

Name	Demo Test
Email	[redacted]@kennasecurity.com
Phone	
Roles	read-only user
Login Count	Never
Last Request	24 days ago
Last Login	Never
API Key	4uorRBNE••••••••

Roles: Roles are fundamental to the Role-based Access Controls (RBAC) within Kenna. In this menu option, you can view and / or modify existing roles, as well as create new ones.



Settings » User Roles » New

Name	
Risk Meters	Search... Grant access to objects that belong to these risk meters
Applications	Search... Grant access to objects that belong to these applications
View Home Page	☑ Disabling will redirect the user's landing page from Home to Explore
View AppSec Reporting	☑ Disabling will remove the user's access to AppSec Reporting pages
Access Type	● Read-only ○ Write ○ Custom Access

Settings » User Roles » Edit

Name	AAE Team
Risk Meters	× AAE Team × Bluekeep Vulnerabilities Grant access to objects that belong to these risk meters
Applications	Select... Grant access to objects that belong to these applications
View Home Page	☑ Disabling will redirect the user's landing page from Home to Explore
View AppSec Reporting	☑ Disabling will remove the user's access to AppSec Reporting pages
Access Type	○ Read-only ○ Write ● Custom Access

Settings » User Roles

Name	Risk Meter Groups	Applications	Permission Level	View Home Page	View AppSec Reporting Page	Actions
AAE Team	AAE Team, Bluekeep Vulnerabilities		custom	Yes	Yes	✎ 🗑
Abbott only role			custom	Yes	Yes	✎ 🗑
AD Windows Admin	Business Unit 3		write	Yes	Yes	✎ 🗑
Anna's Role	2020 Internal Audit, AAE Team, Assets - JAVA - Change Name		custom	Yes	Yes	✎ 🗑
application			read	Yes	Yes	✎ 🗑
BU1	Easy Exploitable		read	Yes	Yes	✎ 🗑
Business Unit User			read	Yes	Yes	✎ 🗑
cisco	Win 7, Assets - JAVA - Change Name		custom	Yes	Yes	✎ 🗑
Compliance			write	Yes	Yes	✎ 🗑
Config Team			write	Yes	Yes	✎ 🗑

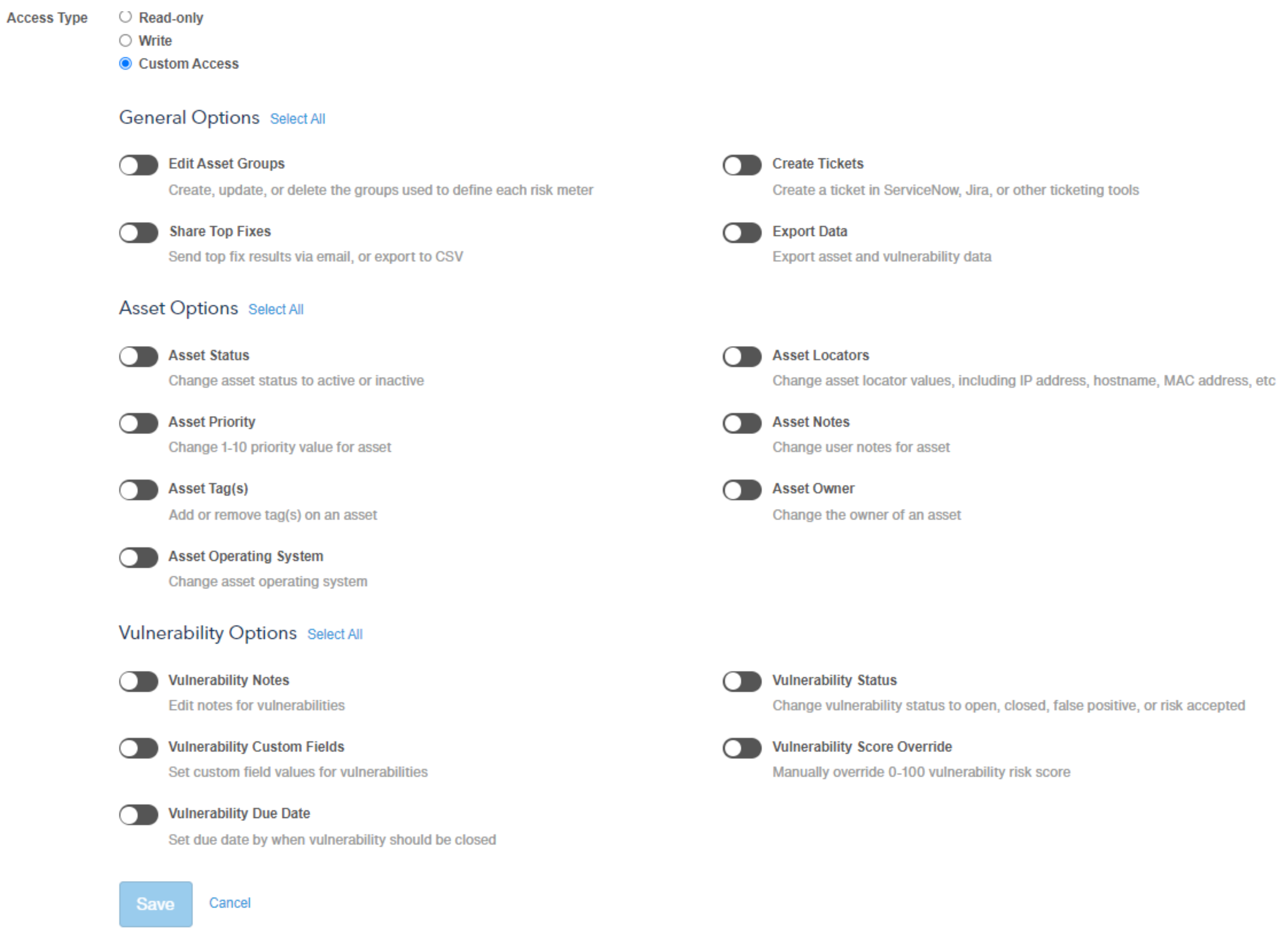
User Roles

There are two system-level roles **administrator** and **normal user**. Custom user roles allow you to create more discrete permission levels.

Roles menu providing interface to view, create and edit roles

The roles feature provides two main functions:

1. Governs access to assets in Kenna: Roles are created with access to applications and Risk Meter groups, and then these roles can then be assigned to individuals to control the access that they have to assets within Kenna. A single user can be assigned as many as 10 roles within Kenna.
2. Access type: Each role can be one of the system roles (read-only, and write), or custom access. This access type regulates the operations that users can perform on assets, vulnerabilities, and Risk Meters within Kenna. Custom access gives more fine-grained options for operations that a user can perform.



Access Type
○ Read-only
○ Write
● Custom Access

General Options Select All

Edit Asset Groups
Create, update, or delete the groups used to define each risk meter

Create Tickets
Create a ticket in ServiceNow, Jira, or other ticketing tools

Share Top Fixes
Send top fix results via email, or export to CSV

Export Data
Export asset and vulnerability data

Asset Options Select All

Asset Status
Change asset status to active or inactive

Asset Locators
Change asset locator values, including IP address, hostname, MAC address, etc

Asset Priority
Change 1-10 priority value for asset

Asset Notes
Change user notes for asset

Asset Tag(s)
Add or remove tag(s) on an asset

Asset Owner
Change the owner of an asset

Asset Operating System
Change asset operating system

Vulnerability Options Select All

Vulnerability Notes
Edit notes for vulnerabilities

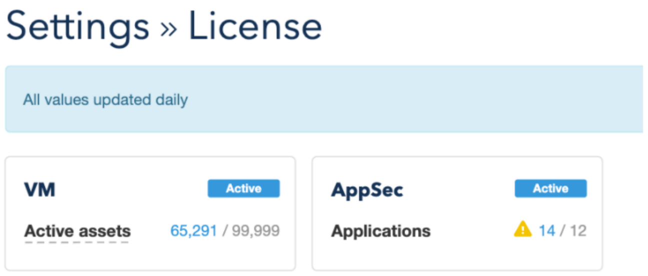
Vulnerability Status
Change vulnerability status to open, closed, false positive, or risk accepted

Vulnerability Custom Fields
Set custom field values for vulnerabilities

Vulnerability Score Override
Manually override 0-100 vulnerability risk score

Vulnerability Due Date
Set due date by when vulnerability should be closed

Licenses: Administrators can get a view of their license information from this menu. This will display your license count and the number of licenses you are using as you see below. These values are calculated daily. An exclamation point means you are over your license counts.



Settings » License

All values updated daily

VM Active
Active assets 65,291 / 99,999

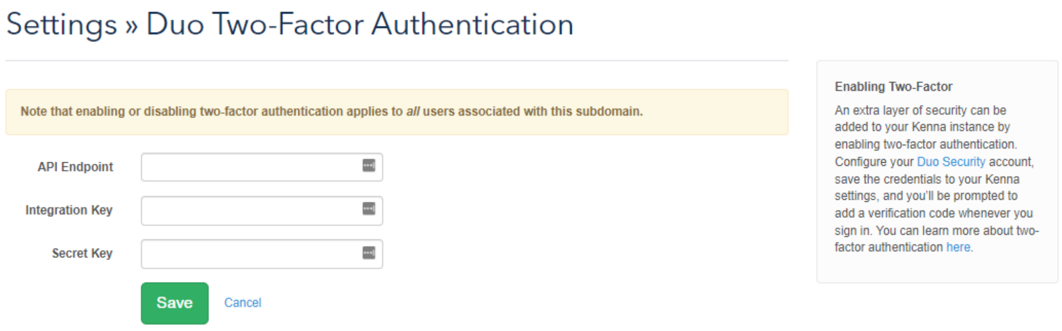
AppSec Active
Applications ⚠ 14 / 12

Custom Fields: While Kenna has a lot of fields that hold relevant information at the vulnerability level (like risk score, name, description, etc.), it also allows for the addition of custom fields. These custom fields can be used to add additional metadata at the vulnerability level. Such metadata can include things like a date a risk was accepted, who accepted a risk, an identifier from external platforms such as a Governance, Risk & Compliance (GRC) platform etc., and can help organizations create and manage workflows within Kenna.

Custom fields can be Text, Date or Numeric. It is important to note that these field-types are more to assist with data-entry and will eventually get stored as a string.

In addition, any created custom field can be setup to show up as a filter option in the VM Explore page. Using custom fields as a filter in the Explore page is not recommended when the filter will return too many unique results as this could impact user performance and/or usability. This help page provides a lot of detail for creating and editing custom fields - https://help.kennasecurity.com/hc/en-us/articles/201921738-Creating-a-Custom-Field.

2FA (Two-factor Auth): The Kenna platform offers the possibility of improved security for an organization through the use of two-factor authentication (2FA). Any user attempting to login to the platform is then prompted for an additional code. Kenna supports only Duo 2FA at this time.



Settings » Duo Two-Factor Authentication

Note that enabling or disabling two-factor authentication applies to *all* users associated with this subdomain.

API Endpoint

Integration Key

Secret Key

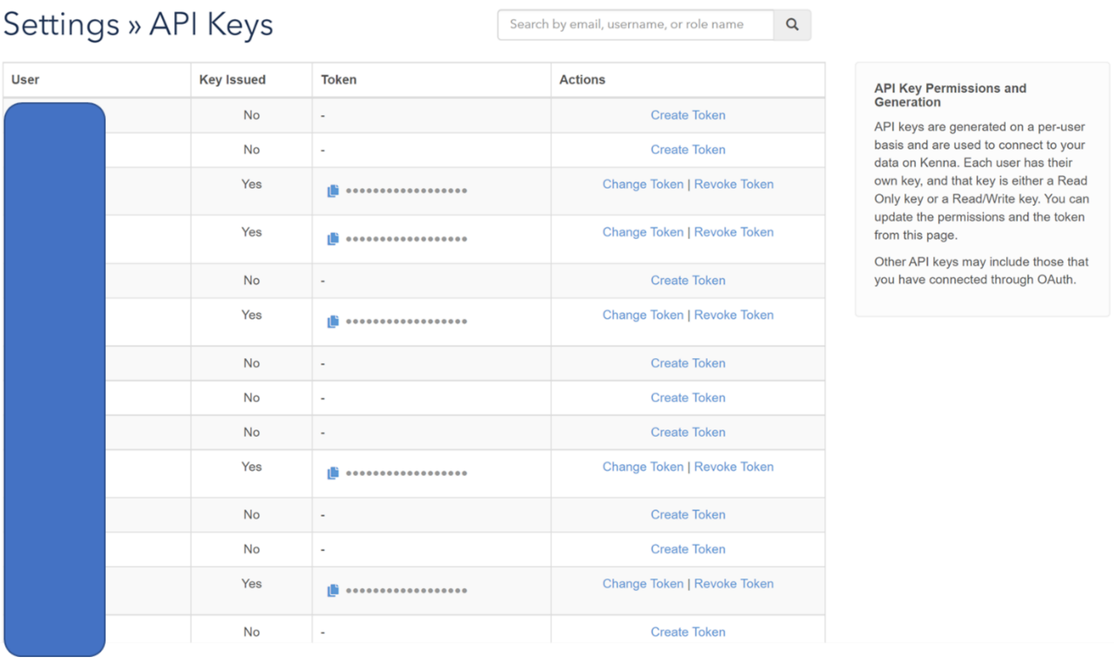
Enabling Two-Factor

An extra layer of security can be added to your Kenna instance by enabling two-factor authentication. Configure your Duo Security account, save the credentials to your Kenna settings, and you'll be prompted to add a verification code whenever you sign in. You can learn more about two-factor authentication here.

A detailed guide for setting up 2FA can be found on this page - https://help.kennasecurity.com/hc/en-us/articles/204368699.

API Keys: Kenna offers a robust API for interacting with the Kenna platform. For a user to make API calls, an API key4 must be generated for that user and then submitted with each API request. The API keys settings menu provides a view into seeing which users have API keys, and an interface for creating, generating, and revoking API keys. At this moment, API keys can only be used by system roles (administrator, read-only, and write roles).

For more information on usage of the API, please see the ***API Operations*** section.



Settings » API Keys

User	Key Issued	Token	Actions
[redacted]	No	-	Create Token
[redacted]	No	-	Create Token
[redacted]	Yes	••••••••••••••••••	Change Token | Revoke Token
[redacted]	Yes	••••••••••••••••••	Change Token | Revoke Token
[redacted]	No	-	Create Token
[redacted]	Yes	••••••••••••••••••	Change Token | Revoke Token
[redacted]	No	-	Create Token
[redacted]	No	-	Create Token
[redacted]	No	-	Create Token
[redacted]	Yes	••••••••••••••••••	Change Token | Revoke Token
[redacted]	No	-	Create Token
[redacted]	No	-	Create Token
[redacted]	Yes	••••••••••••••••••	Change Token | Revoke Token
[redacted]	No	-	Create Token

API Key Permissions and Generation

API keys are generated on a per-user basis and are used to connect to your data on Kenna. Each user has their own key, and that key is either a Read Only key or a Read/Write key. You can update the permissions and the token from this page.

Other API keys may include those that you have connected through OAuth.

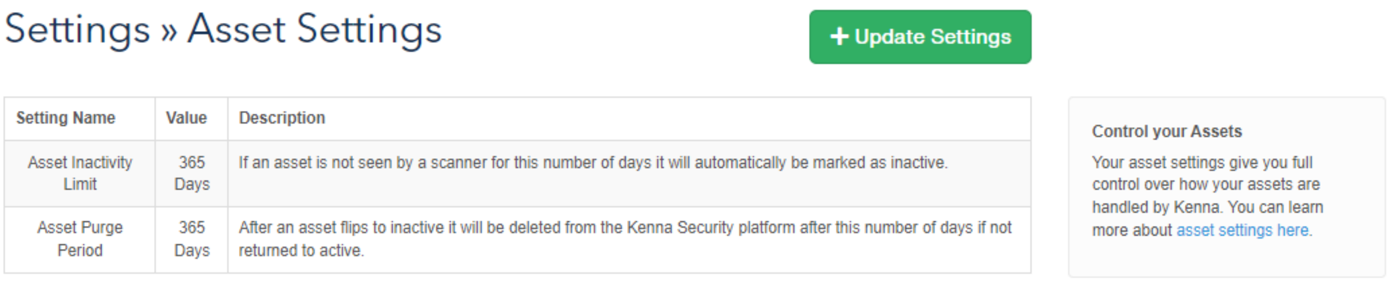
Asset Settings: Assets may persist in Kenna even after we are no longer receiving new vulnerability information about them from your scanner. To remove such stale assets' risk scoring and fix information, they must be set to "inactive" in Kenna. Inactive assets are removed from Risk Meter scoring, will not appear in any default reporting, and will not appear in any fix asset lists. Kenna will automatically flip such inactive assets back to 'active' if the assets are processed as part of a connector run.

If inactive assets remain in the system after a pre-set purge time has elapsed, then those assets are purged from the platform, and if such assets are brought in by subsequent connector runs, then they are treated as new assets.

The Asset settings within Kenna help Kenna to automatically manage the status and presence of assets within Kenna. This is automatically managed on the Global level using the two settings provided within the asset settings page.

Asset Inactivity Limit: This setting defines how long it takes for an asset to be marked as inactive after it hasn't been seen in any connector runs within Kenna.

Asset Purge Period: Once an asset has been marked as inactive, and the configured Asset Purge period has elapsed without the asset being seen, that asset is purged from the Kenna platform.



Settings » Asset Settings

Setting Name	Value	Description
Asset Inactivity Limit	365 Days	If an asset is not seen by a scanner for this number of days it will automatically be marked as inactive.
Asset Purge Period	365 Days	After an asset flips to inactive it will be deleted from the Kenna Security platform after this number of days if not returned to active.

Control your Assets

Your asset settings give you full control over how your assets are handled by Kenna. You can learn more about asset settings here.

Please note the following:

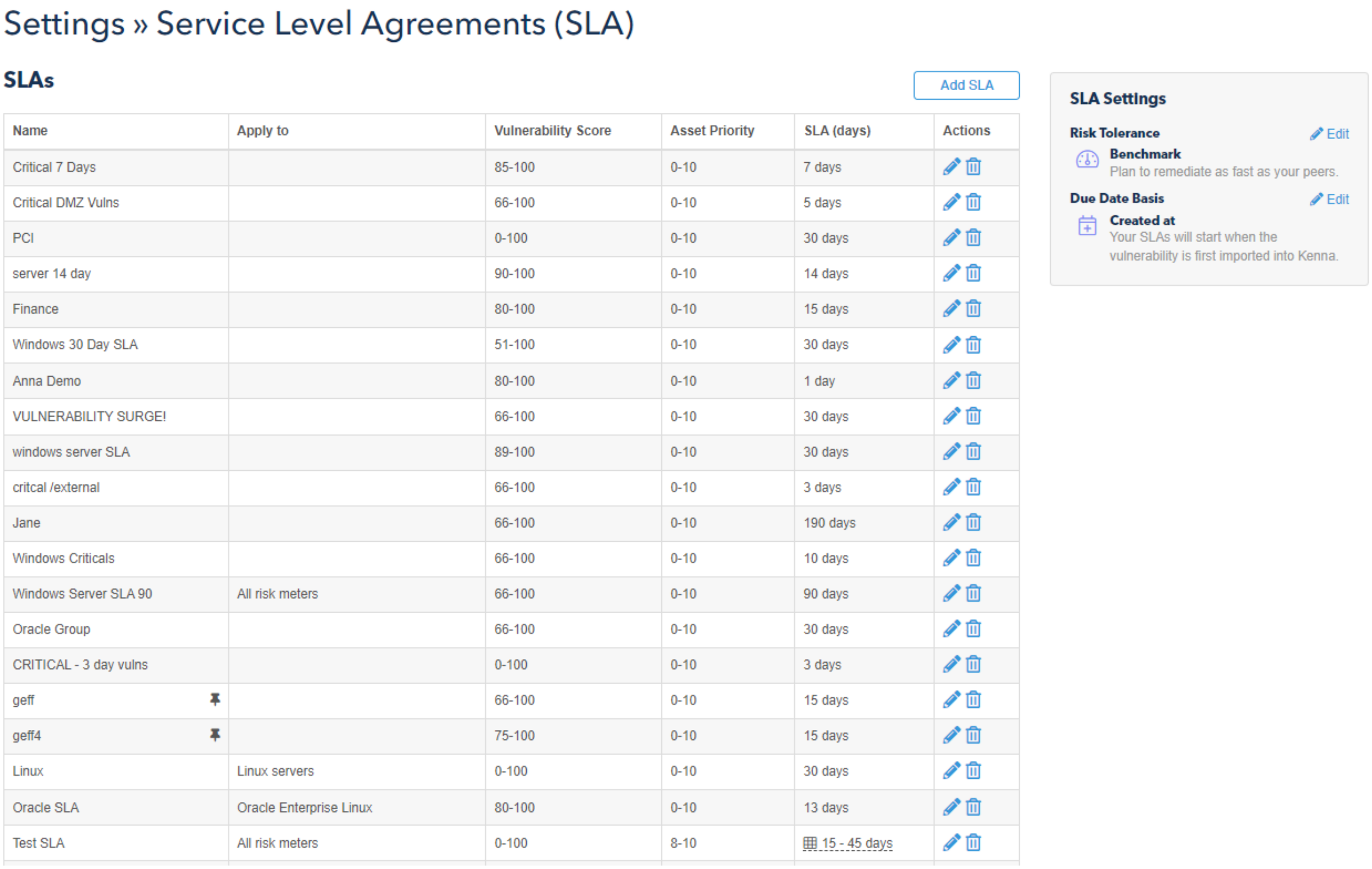
- Assets whose statuses have been manually set by a user will no longer be automatically managed by Kenna, until the ‘Remove override’ feature is used.
- Asset inactivity can also be set at the connector-level under a connector setting. Connector-level asset inactivity settings take precedence over the Global asset inactivity setting.

SLAs: The SLA settings page is an incredibly important one as it helps organizations set SLAs based on one or more of the following Kenna objects:

1. Vulnerability / risk score
2. Asset priority
3. Risk Meter group (assets contained can be any of the possible filters/queries available for Risk Meter creation)

The SLA engine runs every night, and on each run, it evaluates all vulnerabilities that do not have a due date set, and for each evaluation, every set SLA rule is considered, starting from the most aggressive SLAs. If the vulnerability satisfies the condition for the SLA, then the due date is calculated for that vulnerability according to the applicable SLA rule.

The SLA settings menu provides the interface to create new SLAs, modify existing SLAs or delete existing SLAs.



Settings » Service Level Agreements (SLA)

SLAs

Add SLA

Name	Apply to	Vulnerability Score	Asset Priority	SLA (days)	Actions
Critical 7 Days		85-100	0-10	7 days	✎ 🗑
Critical DMZ Vulns		66-100	0-10	5 days	✎ 🗑
PCI		0-100	0-10	30 days	✎ 🗑
server 14 day		90-100	0-10	14 days	✎ 🗑
Finance		80-100	0-10	15 days	✎ 🗑
Windows 30 Day SLA		51-100	0-10	30 days	✎ 🗑
Anna Demo		80-100	0-10	1 day	✎ 🗑
VULNERABILITY SURGE!		66-100	0-10	30 days	✎ 🗑
windows server SLA		89-100	0-10	30 days	✎ 🗑
critcal /external		66-100	0-10	3 days	✎ 🗑
Jane		66-100	0-10	190 days	✎ 🗑
Windows Criticals		66-100	0-10	10 days	✎ 🗑
Windows Server SLA 90	All risk meters	66-100	0-10	90 days	✎ 🗑
Oracle Group		66-100	0-10	30 days	✎ 🗑
CRITICAL - 3 day vulns		0-100	0-10	3 days	✎ 🗑
geff		66-100	0-10	15 days	✎ 🗑
geff4		75-100	0-10	15 days	✎ 🗑
Linux	Linux servers	0-100	0-10	30 days	✎ 🗑
Oracle SLA	Oracle Enterprise Linux	80-100	0-10	13 days	✎ 🗑
Test SLA	All risk meters	0-100	8-10	▦ 15 - 45 days	✎ 🗑

SLA Settings

Risk Tolerance ✎ Edit

Benchmark

Plan to remediate as fast as your peers.

Due Date Basis ✎ Edit

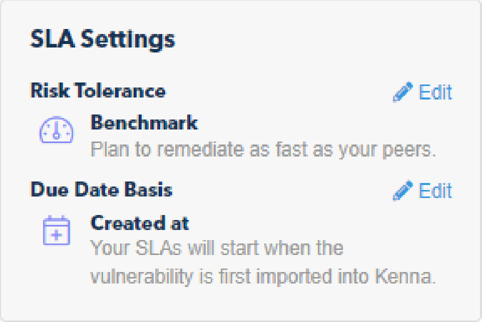
Created at

Your SLAs will start when the vulnerability is first imported into Kenna.

Before any SLA can be set in a Kenna instance, two settings must be set for the organization:

Risk Tolerance: This captures how aggressively an organization plans to remediate vulnerabilities. When SLAs are eventually being configured, this setting is used to recommend the number of days for vulnerabilities based on risk score and asset priority. Three options are presented with detailed description of each.

Due Date Basis: This configures the reference point for the calculation of all due dates. This can be configured as when the vulnerability was first identified by the scanner, when it was first imported into Kenna, or when the vulnerability was first published.



SLA Settings

Risk Tolerance ✎ Edit

Benchmark

Plan to remediate as fast as your peers.

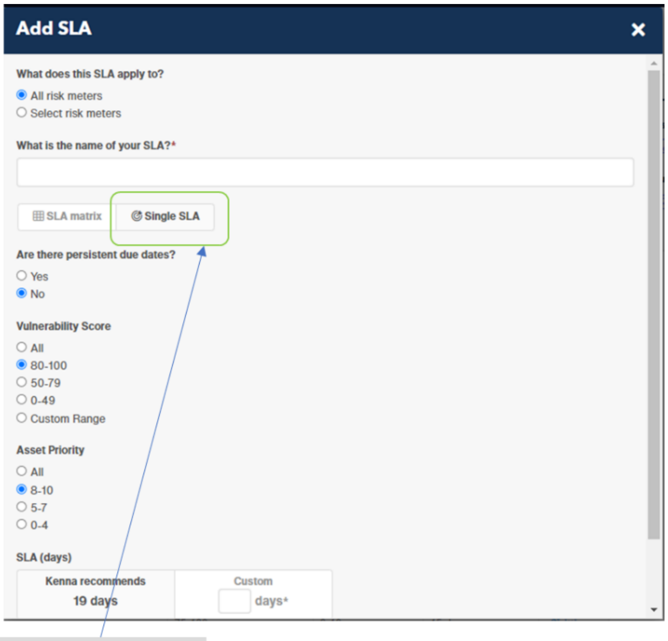
Due Date Basis ✎ Edit

Created at

Your SLAs will start when the vulnerability is first imported into Kenna.

Setting up SLAs

Organizations can either set up individual SLAs, or SLAs in a matrix form, depending on the requirements of the organization. See snippets below which shows the fields to be completed for each type of SLA.



Add SLA

What does this SLA apply to?

● All risk meters
○ Select risk meters

What is the name of your SLA?*

SLA matrix | Single SLA

Are there persistent due dates?

○ Yes
● No

Vulnerability Score

○ All
● 80-100
○ 50-79
○ 0-49
○ Custom Range

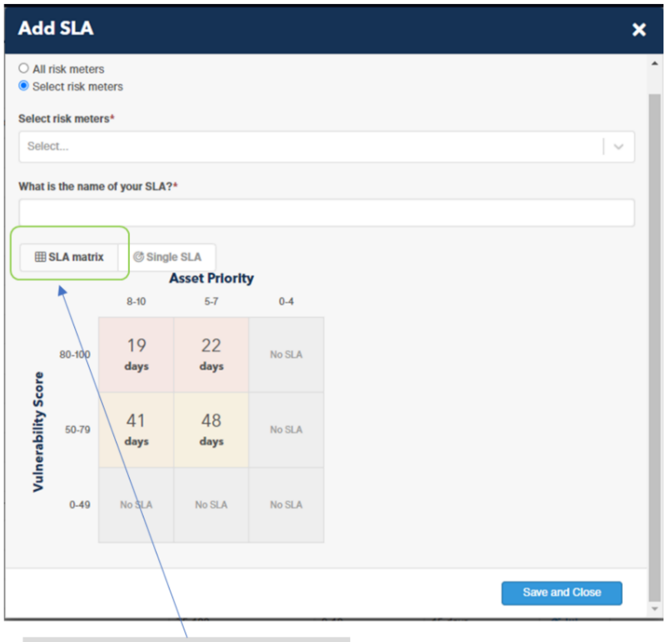
Asset Priority

○ All
● 8-10
○ 5-7
○ 0-4

SLA (days)

Kenna recommends	Custom
19 days	days*

Configuring Single SLA



Add SLA

○ All risk meters
● Select risk meters

Select risk meters*

Select...

What is the name of your SLA?*

SLA matrix | Single SLA

Asset Priority

Vulnerability Score	8-10	5-7	0-4
80-100	19 days	22 days	No SLA
50-79	41 days	48 days	No SLA
0-49	No SLA	No SLA	No SLA

Save and Close

Configuration using SLA matrix

For additional information and reading on the SLA functionality within Kenna, please review the following Help articles.

https://help.kennasecurity.com/hc/en-us/articles/360042683071-Setting-Up-Your-Risk-Based-SLAs and https://help.kennasecurity.com/hc/en-us/articles/211359886-How-do-I-automatically-set-Due-Date-SLA-values-for-my-vulnerabilities-

Upload CSV: This is a legacy method for uploading data into the Kenna platform and is generally not recommended for use. Use the KDI and/or toolkit to upload data from external platforms for which a supported connector has not been built.

API Operations

The Kenna Platform offers a robust API which can be useful for interacting with the platform via automation or scripting. Visit the Kenna API documentation page at ***https://apidocs.kennasecurity.com/reference*** to identify the API base URL that is relevant for your environment.

For a user to get started with making API calls, the user would need to either create an API key (if user is an administrator), or have an administrator create an API key for the user. This API key will be sent as part of each API request that is made. Note that only users that have at least one system role (read, write and administrators) can make API calls at this time. Users with only custom roles are unable to leverage API functionality with their API keys.

The possible operations that a user can make with API calls follow the permissions for the roles for that user (i.e., write operations are not permitted if the user has only read-only access).

This article provides more information on API key generation and permissions - https://help.kennasecurity.com/hc/en-us/articles/360029111331-API-Key-Generation-and-Permissions.

Postman is a popular tool used for interacting with APIs and Kenna has reduced the effort for users getting started with API operations by creating a Postman collection. This collection can be readily imported into Postman and has most of the API calls that are documented in the Kenna Security "API docs" page. The Postman collection is available on the KennaSecurity GitHub page on https://github.com/KennaSecurity/All_Samples/tree/master/postman. The GitHub page gives instructions on how to get started with this Postman collection. For added information on using the Kenna API, as well as setting up the Postman collection, please refer to this blog on the KennaSecurity blog - https://www.kennasecurity.com/blog/postman-collection-api/.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.