Cisco Vulnerability Management

Implementation Success Guide

Contents

What is Cisco Vulnerability Management? 4

Understanding Vulnerability, Asset and Risk Meter Scoring 5

What is a connector? (API vs File-based) 7

Using the Cisco Vulnerability Management Home Page 10

Overview 11

Connector Runs 11

Total Risk Score Over Time 11

Today's Risk Scatterplot 11

Performance Groups 12

News Feed 13

Total Ticket Progress Over Time 13

Other Tab Options From the Home Page 14

Using the VM Dashboard page 15

Filter and Sort Options 15

Card View vs List View 16

Top Fixes 18

Risk Meter Reporting 19

Export and Share Dashboard Reports 19

Create Dashboard Views 20

Set Your Default Dashboard 21

Using the VM Explore page 22

Using Asset Tags 23

Vulnerability Statuses 23

Modify the status of a vulnerability 23

Filter and search for data 24

Create, Edit, and Delete a Risk Meter 26

Create, Edit, and Delete Risk Meters 28

Create a Risk Meter 28

Update a Risk Meter 28

Delete a Risk Meter 29

Create a Child Risk Meter 29

Understanding Vulnerability, Asset and Risk Meter Scoring 30

Fixes and Top Fix Groups 32

Fixes 32

Top Fixes 32
Top Fixes Best Practices 33
Using the Settings menu 35

What is Cisco Vulnerability Management?

Cisco Vulnerability Management is a scalable SaaS solution that leverages real-world exploit data and predictive modeling to provide a real Cisco Security Risk Score of each vulnerability, which helps security teams to prioritize their remediation strategies.

Cisco Vulnerability Management provides the context required to understand the true level of risk that vulnerabilities pose to your organization and equips you with the contextual insight and threat intelligence needed to intercept the next exploit and respond with precision.

Cisco Vulnerability Management ingests, aggregates, and processes billions of pieces of data from internal and external sources, including more than 20 threat and exploit intelligence feeds. Cisco Vulnerability Management then uses proven data science algorithms to automate the analysis of this data and deliver an accurate, quantifiable Cisco Security Risk Score for every vulnerability.

Vulnerability scoring in Cisco Vulnerability Management is designed to create a prioritized order of remediation. The Cisco Security Risk Score considers events happening in real-time for each vulnerability. The score then provides an estimate of the likelihood of exploitation.

For network vulnerabilities, the score is based upon CVE (Common Vulnerabilities and Exposures) and starts with a normalized CVSS (Common Vulnerability Scoring System) score from the National Vulnerability Database. Cisco Vulnerability Management's vulnerability scoring algorithms then assess a wide variety of factors in addition to this score, such as ease of exploitation, active breaches, and popularity as a target, and layers these factors onto that base score to compile a Cisco Security Risk Score.

Understanding Vulnerability, Asset and Risk Meter Scoring

There are three main components of scoring in Cisco Vulnerability Management. Understanding these scoring concepts for vulnerabilities, assets and risk meters will help you use Cisco Vulnerability Management more effectively.

Component 1: Vulnerability Scoring

In Cisco Vulnerability Management, vulnerabilities from your various scanning vendors are imported during connector runs and normalized based on the CVE ID, CWE ID, or the WASC identifier.

For network vulnerabilities, Cisco Vulnerability Management looks at the CVSS base score for the CVE. It then looks at 20+ threat and exploit feeds to understand the volume and velocity of attacks against that CVE, if there is malware available, if it is easy to exploit, whether it is actively being exploited in the wild, and so on. Cisco Vulnerability Management uses all these details help calculate the Vulnerability Score.

For application vulnerabilities, scores are based on the Cisco Security Risk Score from the scanner or a base CWE (Common Weakness Enumeration) score if a scanner score is not available.

Vulnerabilities get a score from 0-100 and are broken into thirds:

- Green 0-33
- Amber 34-66
- Red 67-100

Component 2: Asset Scoring

When Cisco Vulnerability Management calculates the score for an asset, it looks at the highest scored vulnerability present on the asset. Cisco Vulnerability Management considers an asset to be as at risk as its highest vulnerability. This is an important concept to understand because the asset score is not an average based on all the vulnerabilities that are present. As you remediate vulnerabilities on an asset, if you remediate vulnerabilities that are not the highest scored vulnerabilities, the asset score will not change.

Assets get a score from 0-1000 and are broken into thirds and rounded to the nearest 10:

- Green 0-330
- Amber 340-660
- Red 670-1000

The way the default asset score is calculated is to look at the highest scored vulnerability and multiply it by the asset priority. Asset priority is set to 10 by default but is adjustable per asset. For more information on asset priority, refer to Asset Prioritization In Cisco Vulnerability Management or discuss with your CX team.

Highest Vuln Score	X	Asset Priority	=	Default Asset Score
100	X	10	=	1000
80	X	10	=	800
100	X	7	=	700
70	X	6	=	420

Internal vs External IP Scoring

In addition to the default asset score, Cisco Vulnerability Management also applies a 200 point increase in score if the asset has an External IP Address because external facing assets represent a higher risk. Cisco Vulnerability Management, by default, considers any asset with an IP other than a 10.*, 172.16.0.0 -172.31.255.255 and 192.168.* to be an external asset. The highest score will still be 1000 for assets.

Note: This external 200 point increase can be disabled for those customers who use publicly routable IP space internally. For more information, contact your CX team member.

Highest Vuln Score	X	Asset Priority	=	Default Asset Score	External IP?	+	Final Asset Score
100	X	10	=	1000	yes	200	1000
80	X	10	=	800	no	0	800
100	X	7	=	700	yes	200	900
70	X	6	=	420	yes	200	620

Component 3: Risk Meter Score

The last component of scoring is the Risk Meter Score. This score is calculated by taking the average of all the active, non-zero scored assets in the group. Risk Meters are assigned a score between 0-1000 and are broken into thirds and rounded to the nearest 10:

- Green 0-330
- Amber 340-660
- Red 670-1000

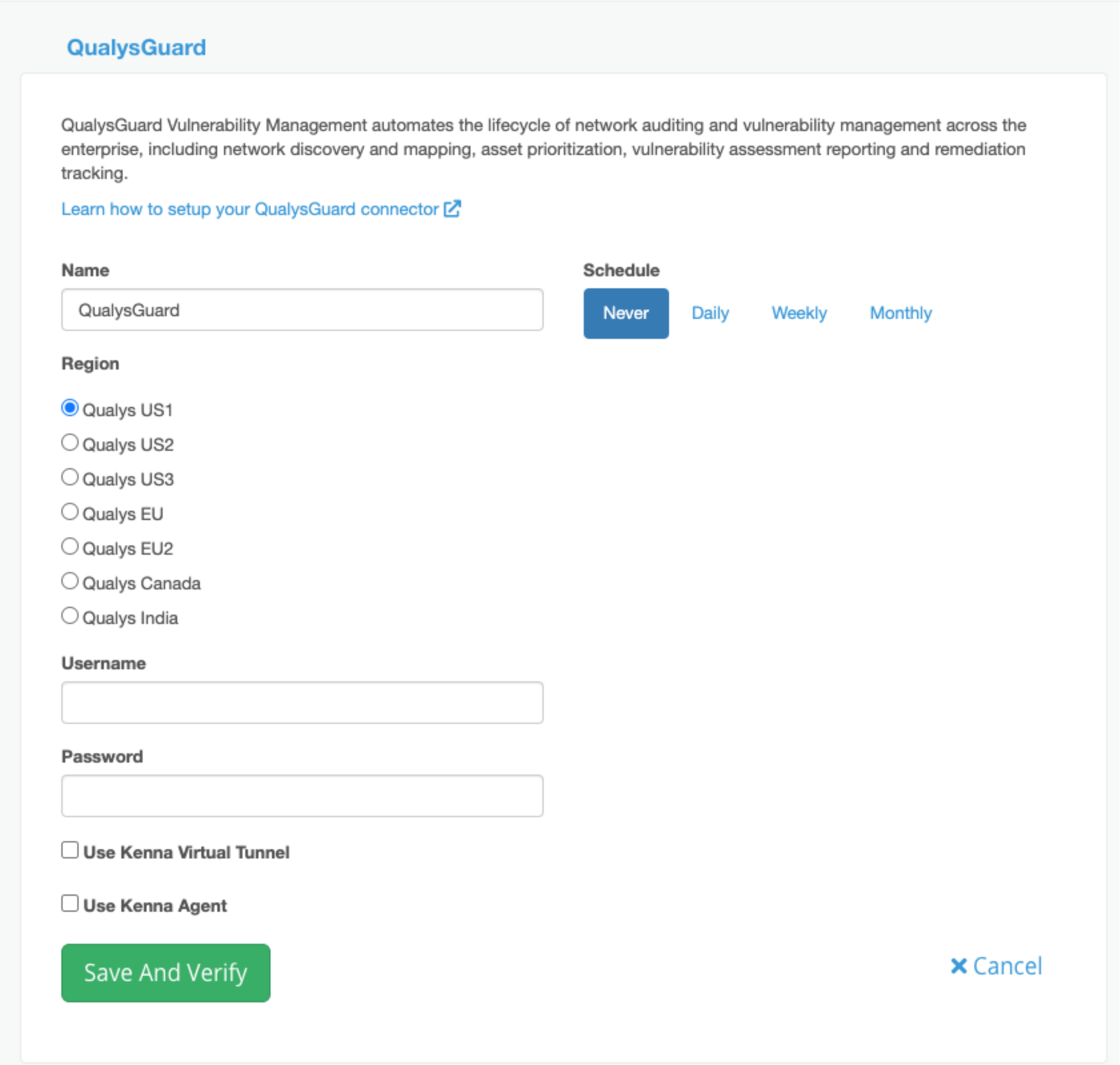
What is a connector? (API vs File-based)

A Connector is how Cisco Vulnerability Management connects to tools that already exist in customer environments. Connectors fall into several general categories and can be related to vulnerability management, application scanning, ticketing, and more. By setting up a connector in your environment, you facilitate a connection between the tool and Cisco Vulnerability Management. The connectors come with a number of settings, including what credentials to use, how often Cisco Vulnerability Management should import the data, and which reports/templates Cisco Vulnerability Management should import,

There are two types of connectors available:

- API Connectors
- File based connectors

API Connectors are direct integrations between Cisco Vulnerability Management and a tool. These integrations are more automated. For these connectors a number of fields can be set to determine what level of data Cisco Vulnerability Management will import and how often you would like that data imported. QualysGuard is an example of an API Connector.



QualysGuard

QualysGuard Vulnerability Management automates the lifecycle of network auditing and vulnerability management across the enterprise, including network discovery and mapping, asset prioritization, vulnerability assessment reporting and remediation tracking.

Learn how to setup your QualysGuard connector

Name: QualysGuard

Schedule: [✓ Never] Daily Weekly Monthly

Region

● Qualys US1
○ Qualys US2
○ Qualys US3
○ Qualys EU
○ Qualys EU2
○ Qualys Canada
○ Qualys India

Username

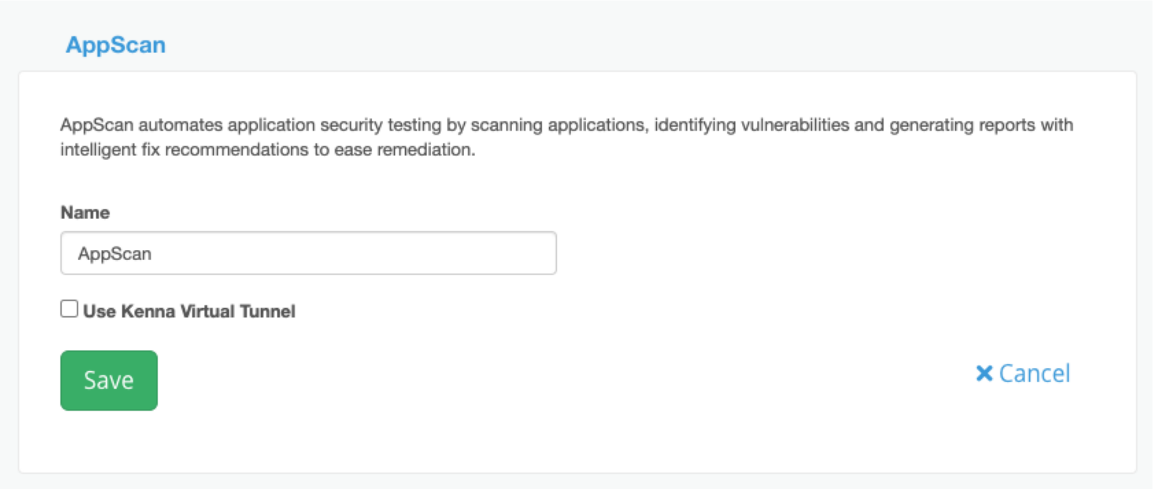
Password

□ Use Kenna Virtual Tunnel

□ Use Kenna Agent

File based connectors are more manual integrations. For file based connectors, Cisco Vulnerability Management supports the creation of a connector, but then a manual drag and drop is required to run the connector. Automation can be achieved through scripting, however you cannot use the Cisco Vulnerability Management UI to schedule a file based connector run.

For example, HCL AppScan is a file based connector (note that Cisco Vulnerability Management does also offer an HCL AppScan Enterprise API connector).



AppScan

AppScan automates application security testing by scanning applications, identifying vulnerabilities and generating reports with intelligent fix recommendations to ease remediation.

Name

AppScan

☐ Use Kenna Virtual Tunnel

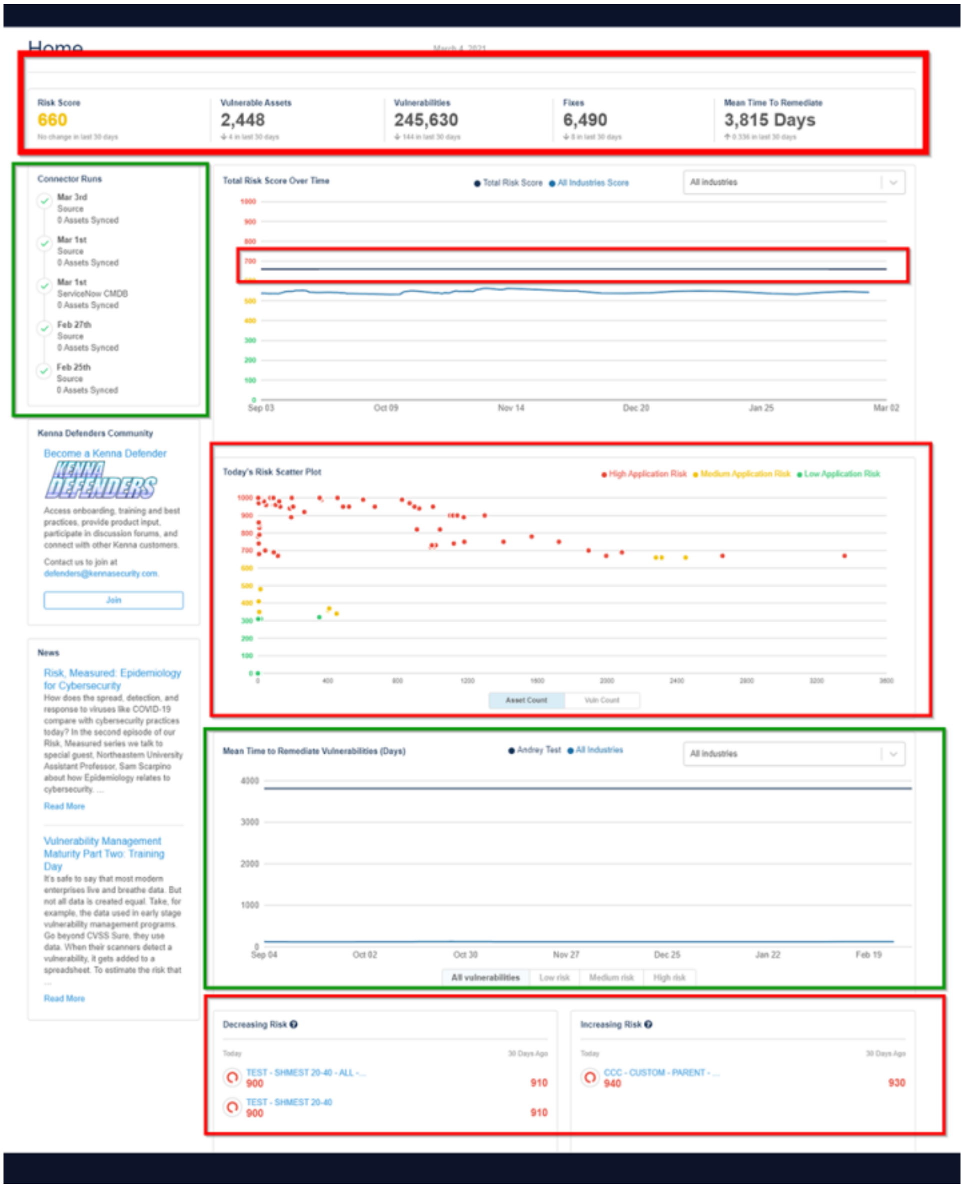
Click here for a full list of tools that Cisco Vulnerability Management can integrate with.

If you don’t see a particular tool on the list and would like to be able to ingest data from that tool, you may be able to do so via the Data Importer. For more details on the Data Importer, refer to the information here.

Using the Cisco Vulnerability Management Home Page

The Home page is a reporting page that reflects full customer data. Users with enough permissions see information for all assets highlighted in the charts and scatterplots.

Note that the user's role can impact how much detailed information is available. In the following image, the sections outlined in red are the ones where Custom Role users will see different numbers compared to users with greater permissions.



Home

March 4, 2021

Risk Score	Vulnerable Assets	Vulnerabilities	Fixes	Mean Time To Remediate
660	2,448	245,630	6,490	3,815 Days
No change in last 30 days	↓ 4 in last 30 days	↓ 144 in last 30 days	↓ 8 in last 30 days	↑ 0.336 in last 30 days

Connector Runs

- ✓ Mar 3rd
Source
0 Assets Synced
- ✓ Mar 1st
Source
0 Assets Synced
- ✓ Mar 1st
ServiceNow CMDB
0 Assets Synced
- ✓ Feb 27th
Source
0 Assets Synced
- ✓ Feb 25th
Source
0 Assets Synced

Kenna Defenders Community

Become a Kenna Defender

KENNA DEFENDERS

Access onboarding, training and best practices, provide product input, participate in discussion forums, and connect with other Kenna customers.

Contact us to join at defenders@kennasecurity.com.

Join

News

Risk, Measured: Epidemiology for Cybersecurity

How does the spread, detection, and response to viruses like COVID-19 compare with cybersecurity practices today? In the second episode of our Risk, Measured series we talk to special guest, Northeastern University Assistant Professor, Sam Scarpino about how Epidemiology relates to cybersecurity. ....

Read More

Vulnerability Management Maturity Part Two: Training Day

It's safe to say that most modern enterprises live and breathe data. But not all data is created equal. Take, for example, the data used in early stage vulnerability management programs. Go beyond CVSS Sure, they use data. When their scanners detect a vulnerability, it gets added to a spreadsheet. To estimate the risk that ...

Read More

Decreasing Risk

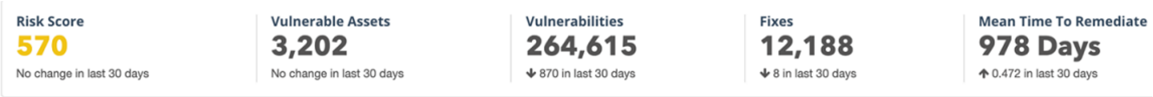
Today	30 Days Ago
TEST - SHMEST 20-40 - ALL -... 900	910
TEST - SHMEST 20-40 900	910

Increasing Risk

Today	30 Days Ago
CCC - CUSTOM - PARENT - ... 940	930

Important: Data that is unavailable to a user with a Custom Role will be greyed-out and the user will not be able to click it. For example, on the "Today's Risk Meter Scatter Plot" users with Custom Roles can click on "Not Accessible" to see inaccessible risk meters represented as grey dots.

Overview



Risk Score	Vulnerable Assets	Vulnerabilities	Fixes	Mean Time To Remediate
570	3,202	264,615	12,188	978 Days
No change in last 30 days	No change in last 30 days	↓ 870 in last 30 days	↓ 8 in last 30 days	↑ 0.472 in last 30 days

Overview is a macro-level view of your organization, where you can find the total Cisco Security Risk Score for your entire business. These statistics are an aggregate view of all active assets and open vulnerabilities, refreshed daily.

Note: Cisco Vulnerability Management processes background jobs, such as risk meter refreshes, between 1 AM and 5 AM local time in EU and AJPC, and between 10:30 and 1:30 in the US region, excluding Hawaii.

Risk Score: The nightly snapshot of the average of all of the active, non-zero scored assets.

Vulnerable Assets: The number of active assets.

Vulnerabilities: The number of open vulnerabilities across active assets.

Fixes: The number of fixes that are available to remediate all of the open vulnerabilities.

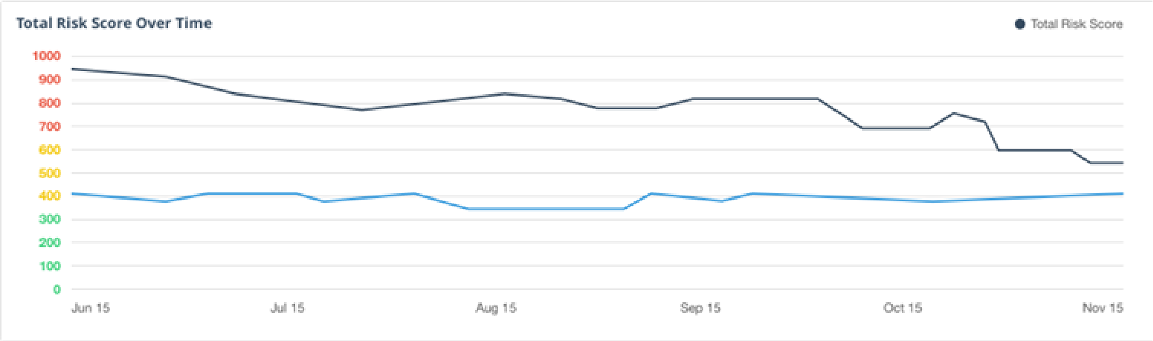
Mean Time To Remediate: The average number of days it takes for you to remediate vulnerabilities.

Connector Runs

You can use the connector run section to track the progress of your connector runs in real-time, and view connector run history.

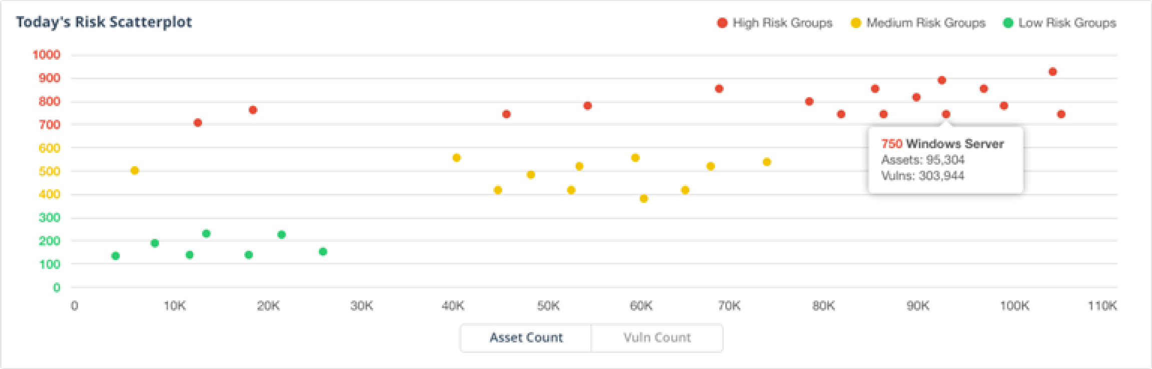
Total Risk Score Over Time

This chart measures total risk from the past to present day. It's a great way to measure your progress. All user roles with permission to view the Home Page can see the Total Risk Score line in the chart.

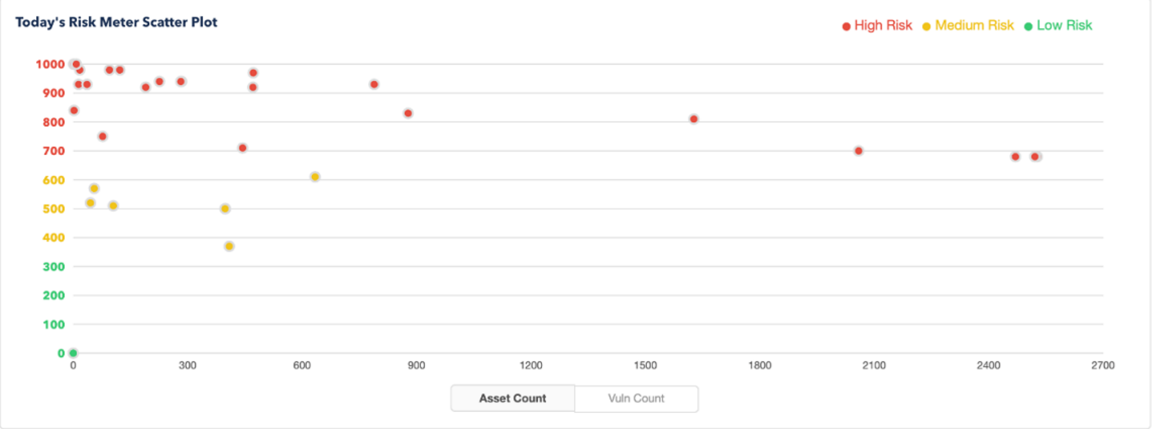


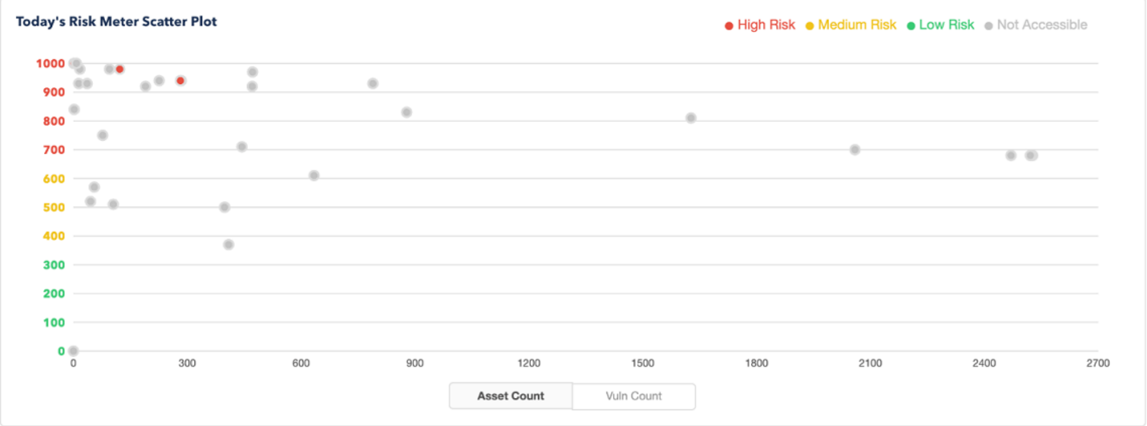
Today's Risk Scatterplot

This all-inclusive chart displays every risk meter you can access. Each dot represents a risk group. The groups are separated by color into low, medium, and high risk. The Asset Count and Vulnerability Count toggle button adjusts the X-axis ranges (minimum value to maximum value).



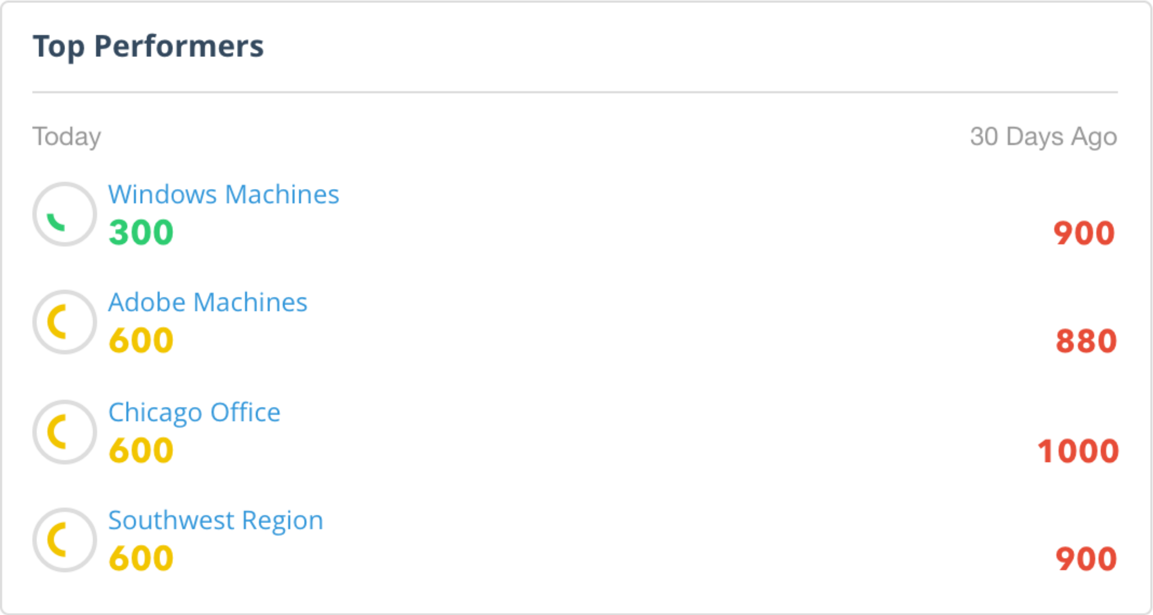
Important: Custom Roles that do not have permission to view certain risk groups will see grey dots in place of the ones with color. You can click the legend to filter the Not Accessible risk meters.





Performance Groups

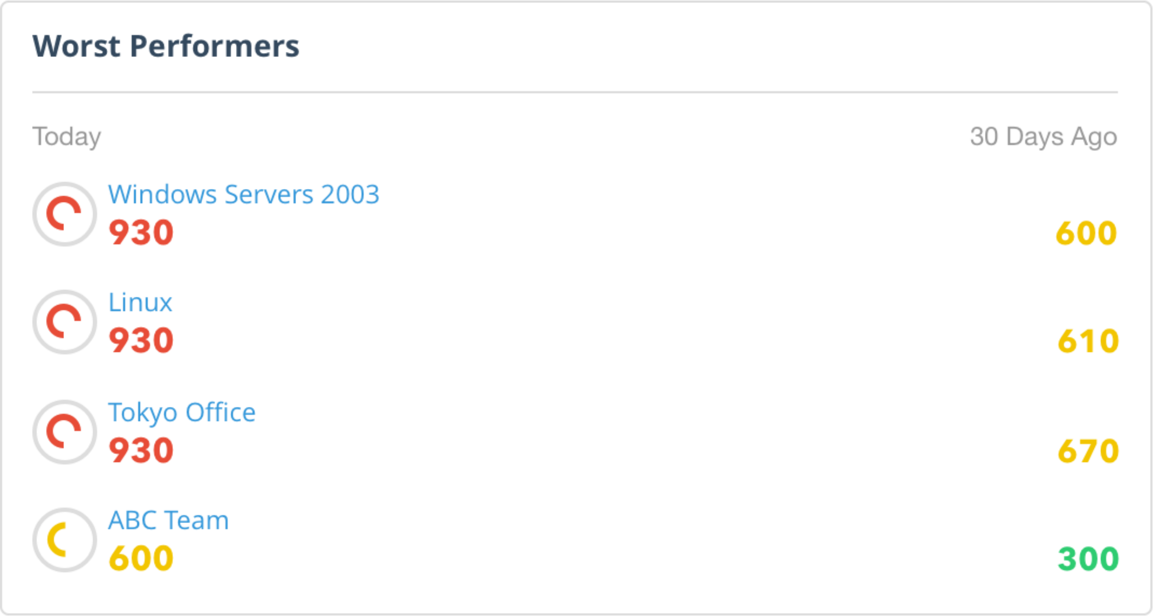
The **Top Performers** section shows your risk groups that have the greatest Cisco Security Risk Score reduction in the last 30 days.



Top Performers

Today	30 Days Ago
Windows Machines 300	900
Adobe Machines 600	880
Chicago Office 600	1000
Southwest Region 600	900

The **Worst Performers** section shows your risk groups with the least Cisco Security Risk Score reduction.



Worst Performers

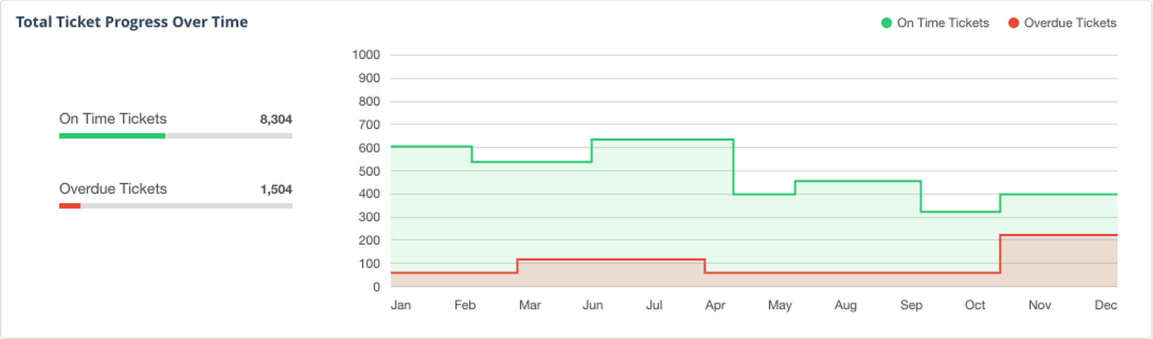
Today	30 Days Ago
Windows Servers 2003 930	600
Linux 930	610
Tokyo Office 930	670
ABC Team 600	300

News Feed

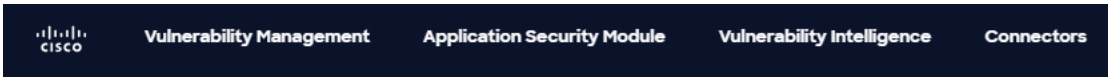
This section helps you stay up to date with the latest from Cisco Vulnerability Management executives, data scientists and subject matter experts with a feed from the Cisco Vulnerability Management blog.

Total Ticket Progress Over Time

If you have integrated a ticket system with Cisco Vulnerability Management, this graph will show all of your tickets by status (On Time and Overdue).



Other Tab Options From the Home Page



VM

You can hover over the VM tab and choose from the Dashboard, Explore or Activity pages. On the Dashboard page you can see all of the risk meters you have access to, and any dashboard views you have set up. On the Explore page you can see the live view for all your data. Here, you can filter and interact with your assets, vulnerabilities, and fixes. On the Activity page you can see an overview of your risk group activity including reports.

AppSec

You can hover over the AppSec tab and choose from the Dashboard, Explore, Reporting, or Stacks pages. On the Dashboard page you can see all the Application Security Module applications that have been configured in your instance. On the Explore page you can discover findings by application, searching, or using dynamic filters. On the Reporting page you can see the overall Reporting summary for all your Application Security Module applications. On the Stacks page you can organize your risk groups and applications into a single view.

VI

You can hover over the VI tab and choose from the Dashboard or Explore pages for the Vulnerability Intelligence offering. On the Dashboard page you can view the top vulnerabilities for multiple categories in a quick view dashboard. On the Explore page you can discover, browse, and search the Cisco Vulnerability Management vulnerability database to understand key vulnerability details, compare CVSS scores, and benchmark them against Cisco Vulnerability Management's scoring algorithm.

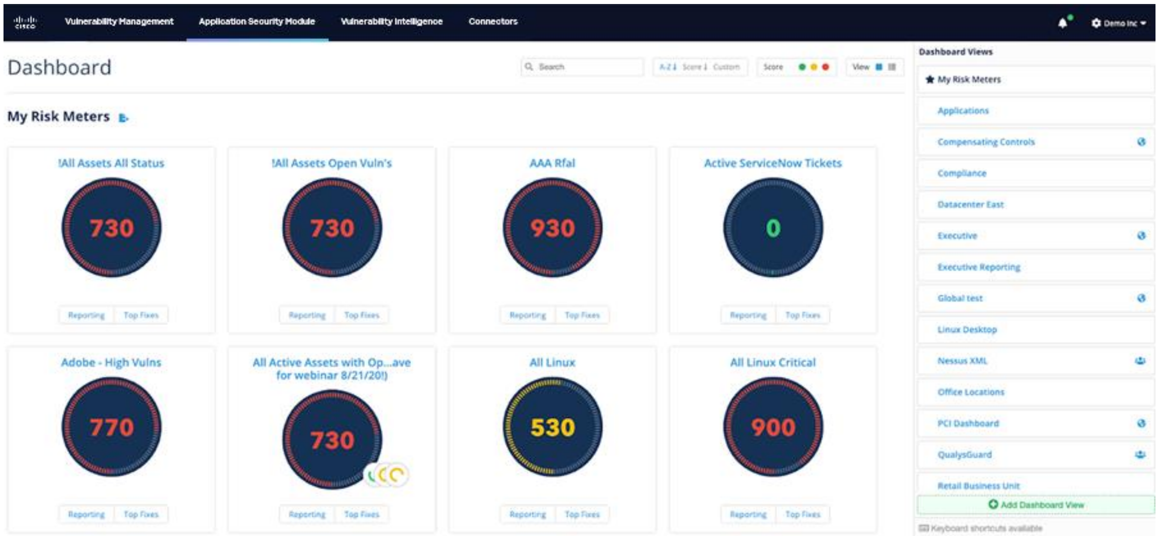
Connectors

That Connectors menu item allows you administrative access to Connector functions and lists.

Using the VM Dashboard page

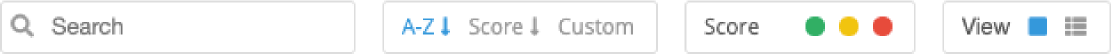
The VM Dashboard page allows you to group your Risk Meters into views specific to your audience or needs. When you open the dashboard page, your Default Dashboard View and all your Risk Meters display. To create risk groups, navigate to the VM > Explore page.

The dashboard is role-based access control (RBAC) dependent, so only Risk Meters you have access to will display.



Filter and Sort Options

You can use the various search and sort options to help organize your Risk Meters in a way that makes sense for your organization.



You can use these options to quickly:

- search for Risk Meters
- organize Risk Meters in alphabetical/reverse alphabetical order
- organize using the Score (low to high; high to low)
- select the green, yellow, and red dots to remove risk meters of that score range from view.

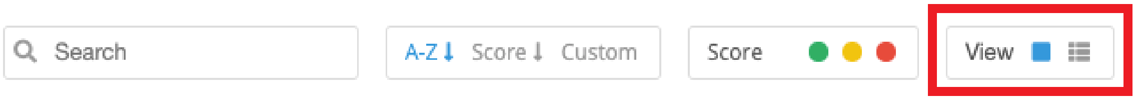
The Risk Meter score and color scheme provide an easy way to focus on Asset Groups that pose the highest risk to your organization. Each risk meter is assigned a Cisco Security Risk Score, which comes with a correlating color:

- Green = Risk Meter score between 0-333
- Yellow/Amber = Risk Meter score between 334-666

- Red = Risk Meter score between 667-1000

Card View vs List View

There are two ways to view the risk groups on the Dashboard page: card view and list view.



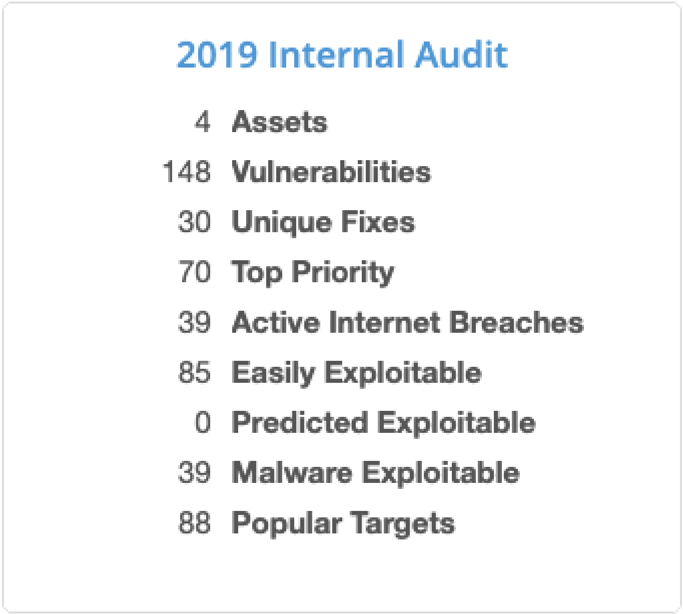
Card View

Card view allows you to view the Risk Meter dial and score, and has buttons to access the Reporting or Top Fixes pages.

- If you click Reporting, a page displays that shows your trending risk over time.
- If you click Top Fixes, a page displays that shows top fixes for the risk meter.

From the Card View, you can view all your risk meters including icons that indicate the presence of descendant meters (you can create risk groups which descend or inherit their filters and search criteria). Clicking a Child icon opens a new window that displays the children of the parent risk meter. Continue clicking Child icons to move through any child risk meters.

You can click the ‘i” key on your keyboard to bring up the Risk Group Overview for that Risk Meter where you can see the count of items such as assets, vulnerabilities, and unique fixes.



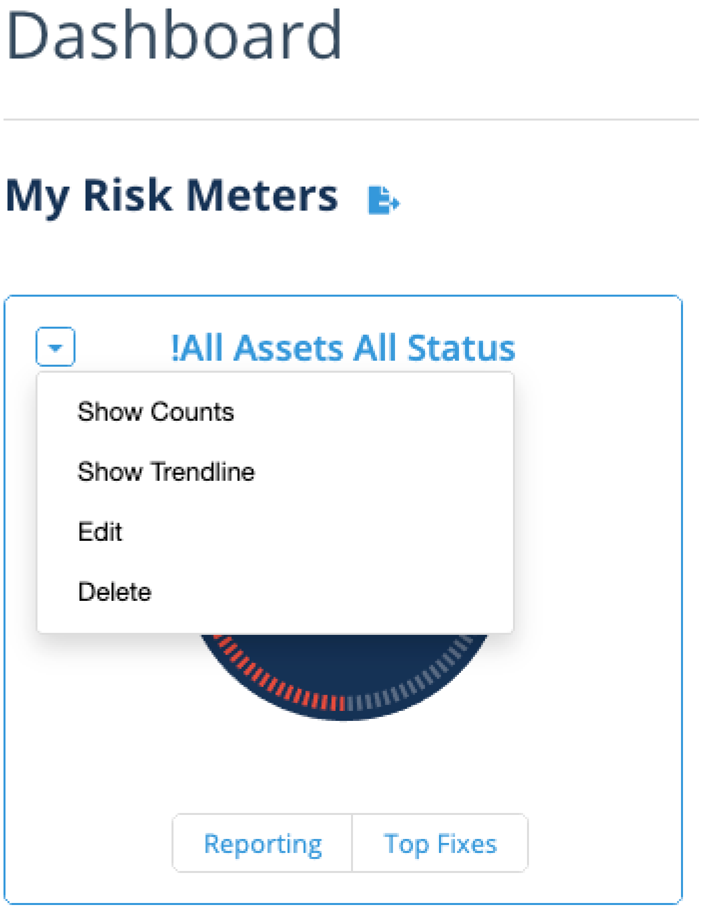
2019 Internal Audit

4	Assets
148	Vulnerabilities
30	Unique Fixes
70	Top Priority
39	Active Internet Breaches
85	Easily Exploitable
0	Predicted Exploitable
39	Malware Exploitable
88	Popular Targets

- **Assets** - the number of assets included in the group
- **Vulnerabilities** - the number of vulnerabilities that exist on those assets

- **Unique Fixes** - the number of unique patches outstanding for the vulnerabilities on the assets contained in the Risk Meter
- **Top Priority** - the number of Top Priority vulnerabilities within the overall vulnerability count
- **Active Internet Breaches** - the number of vulnerabilities within the group that are part of Active Internet Breach activity in the wild
- **Easily Exploitable** - the number of vulnerabilities within the group or which there are known exploit kits
- **Predicted Exploitable** - the number of vulnerabilities predicted to become exploitable
- **Malware Exploitable** - the number of vulnerabilities actively exploited with Malware including Trojans, Worms, Ransomware, and more
- **Popular Targets** - the number of vulnerabilities that are also seen in high volume by other Cisco Vulnerability Management clients

If you hover over the Risk Meter name and click the arrow icon, additional options display:



- **Show Counts** provides a Risk Group Overview, which is the same as clicking the “i” key on your keyboard.

- **Show Trendline** changes the score dial into a trendline which displays the last 90 days performance for that Risk Meter.
- **Edit** allows you to edit the name of the Risk Meter, and which roles have access. Or you can go to the Explore page to edit the criteria for the Risk Meter.
- **Delete** allows you to delete the Risk Meter.

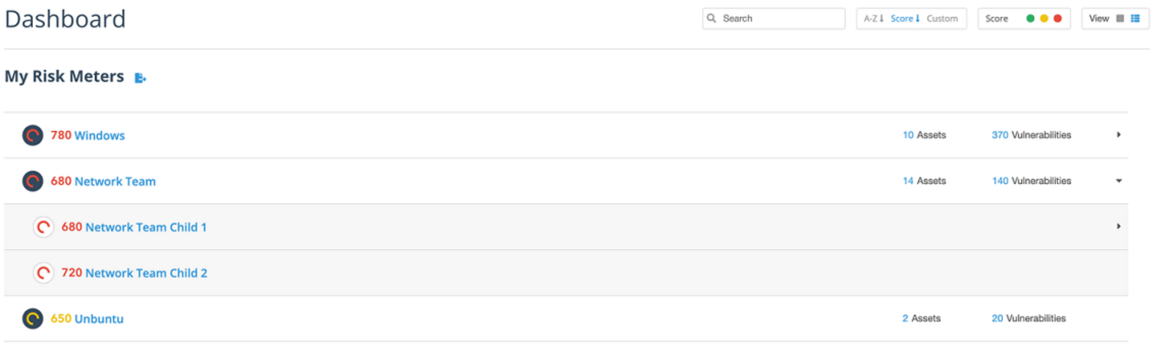
  Note This is a permanent action and cannot be undone! This will delete the risk meter entirely from Cisco Vulnerability Management, not just the Dashboard page.

List View

List view allows you to view a list of your Risk Meters instead of the score dial. The number of assets and vulnerabilities for each group display along with the score. You can also hover over the name of the Risk Meter to display the Reporting, Top Fixes, Edit and Delete actions.

You can also view descendant risk meters in the List View. The risk meters appear, which allow you to expand and collapse risk groups.

In the List View, you can access the Assets and Vulnerabilities links, which open in the Explore window.

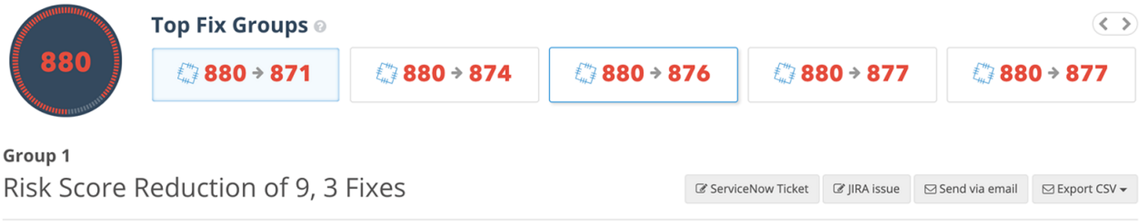


My Risk Meters

780 Windows	10 Assets	370 Vulnerabilities
680 Network Team	14 Assets	140 Vulnerabilities
680 Network Team Child 1		
720 Network Team Child 2		
650 Unbuntu	2 Assets	20 Vulnerabilities

Top Fixes

For each risk group, Cisco Vulnerability Management provides Top Fixes. To access the top fixes, on the VM Dashboard page, navigate to the risk meter that you want to see the top fixes for and click the Top Fixes button. Each Top Fix is a group of up to 3 fixes that fall in the top 10 largest risk reductions for that Risk Meter. The Top Fix view for a Risk Meter contains its current Cisco Security Risk Score, along with the lower score that the Risk Meter would move to after remediating all vulnerabilities in a specific Fix Group. These are sorted by largest risk reduction, left to right, with a button on the right side to move to the second page of Top Fixes.



Group 1

Risk Score Reduction of 9, 3 Fixes

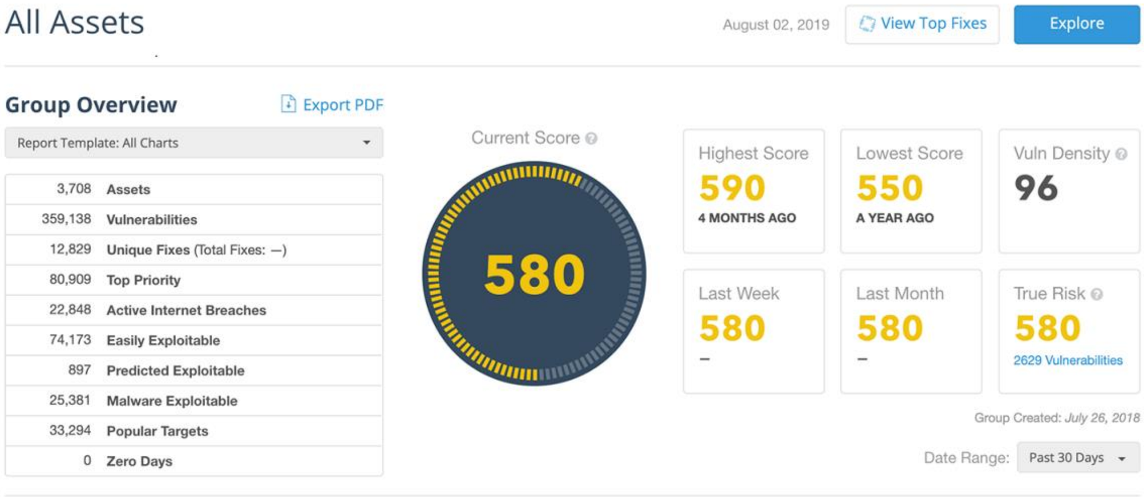
Risk Meter Reporting

Risk Meter reports visualize your trending risk over time. As soon as a Risk Meter or Asset Group is created in Cisco Vulnerability Management, nightly captures of data begin to create the metric displayed in the report. To access a report, click on the Reporting button in the bottom left-hand corner of any Risk Meter on the Dashboard.

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 might see changes in asset and vulnerability counts in the reports. Also, if you delete a risk meter, you will delete all historical data previously collected for that meter.

The Risk Group Overview section shows general counts and captures Risk Group scores over time and a vulnerability density count. Use the "Export PDF" link at the top of this section to download a PDF version of the full report. In the bottom right-hand corner, you will see the True Risk score if you have accepted risk for any vulnerabilities in this group.



All Assets

August 02, 2019

Group Overview

Report Template: All Charts

3,708	Assets
359,138	Vulnerabilities
12,829	Unique Fixes (Total Fixes: —)
80,909	Top Priority
22,848	Active Internet Breaches
74,173	Easily Exploitable
897	Predicted Exploitable
25,381	Malware Exploitable
33,294	Popular Targets
0	Zero Days

Current Score: 580

Highest Score: 590, 4 MONTHS AGO

Lowest Score: 550, A YEAR AGO

Vuln Density: 96

Last Week: 580 –

Last Month: 580 –

True Risk: 580, 2629 Vulnerabilities

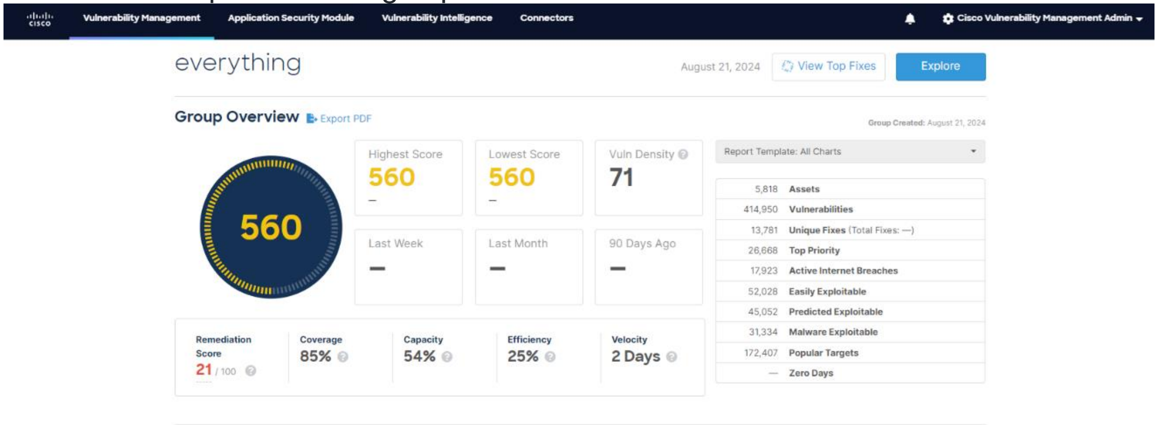
Group Created: July 26, 2018

Date Range: Past 30 Days

Export and Share Dashboard Reports

1. You can also generate high-level dashboard reports that you can share.
2. On the VM Dashboard page, in the Asset Group that you want a report for, click **Reporting**.
   A report displays that shows various remediation and risk exposure information

related to that specific asset group.



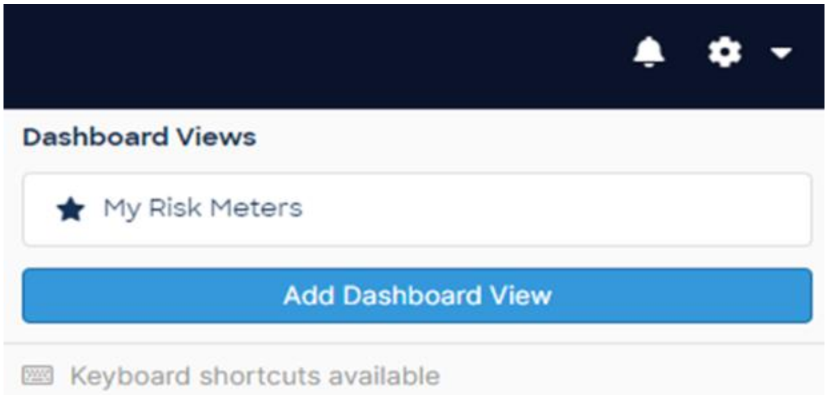
5,818	Assets
414,950	Vulnerabilities
13,781	Unique Fixes (Total Fixes: —)
26,668	Top Priority
17,923	Active Internet Breaches
52,028	Easily Exploitable
45,052	Predicted Exploitable
31,334	Malware Exploitable
172,407	Popular Targets
—	Zero Days

3. Click **Export PDF > Print**.
4. Save the PDF.

Create Dashboard Views

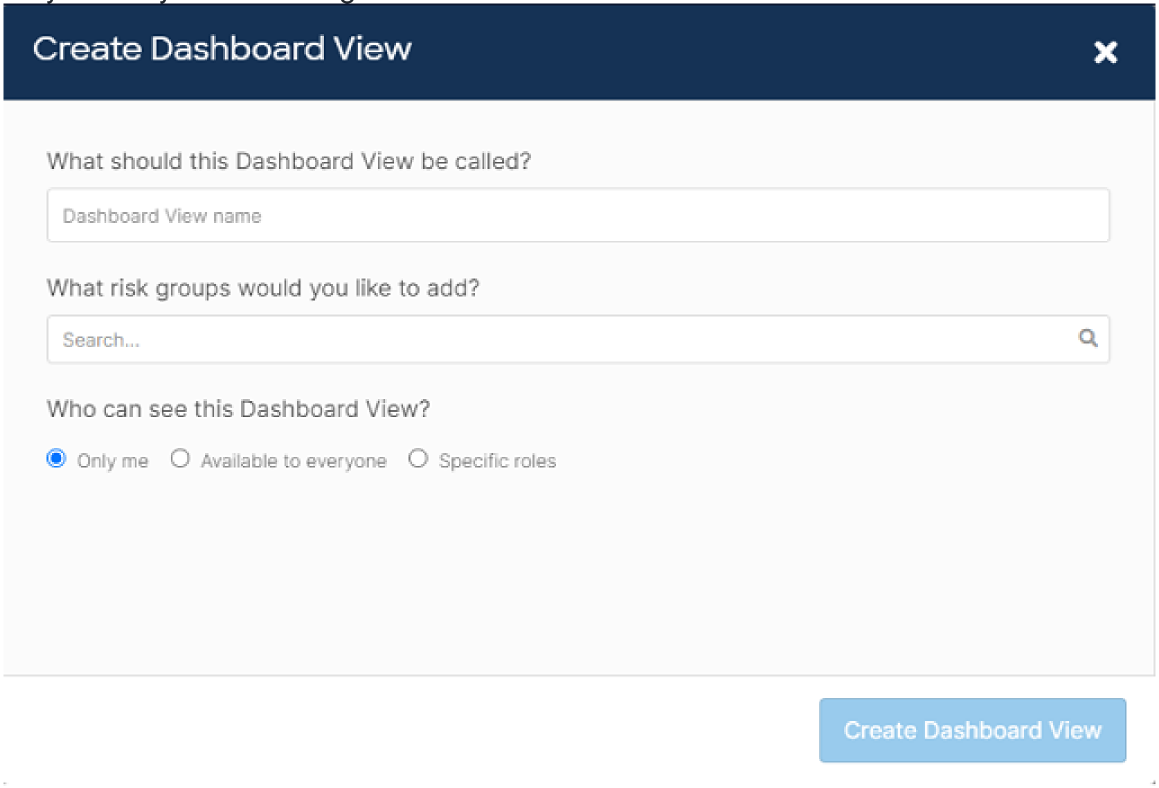
You can create additional Dashboard Views which contain subsets of your Risk Groups.

1. Click **Add Dashboard View**.



2. In the Create Dashboard View page, enter a Name, the risk meters that you want to include in the dashboard view, and who can see the dashboard. **Note**: Client administrators can create Global and Shared dashboard views. They can be made available to everyone (Global) or limited to specific user roles (Shared). The risk meters visible to a specific user on a shared dashboard are determined by the role-based access controls (RBAC) in place. If a shared dashboard has 10 risk meters on it but the specific user only has permission to see eight of them, then

they will only see those eight.



Create Dashboard View ✕

What should this Dashboard View be called?

Dashboard View name

What risk groups would you like to add?

Search...

Who can see this Dashboard View?

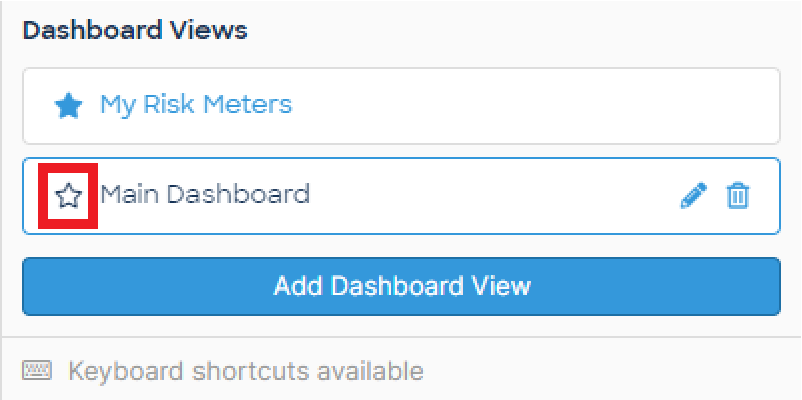
● Only me ○ Available to everyone ○ Specific roles

3. Click **Save Dashboard View**.

Set Your Default Dashboard

You can designate your own default dashboard. It can be one you created yourself or it can be a global/shared dashboard that an administrator created. This default dashboard will display each time you log into Cisco Vulnerability Management (after logging out) and open the Dashboard page.

To choose a Dashboard as your default, click on the star next to its name.



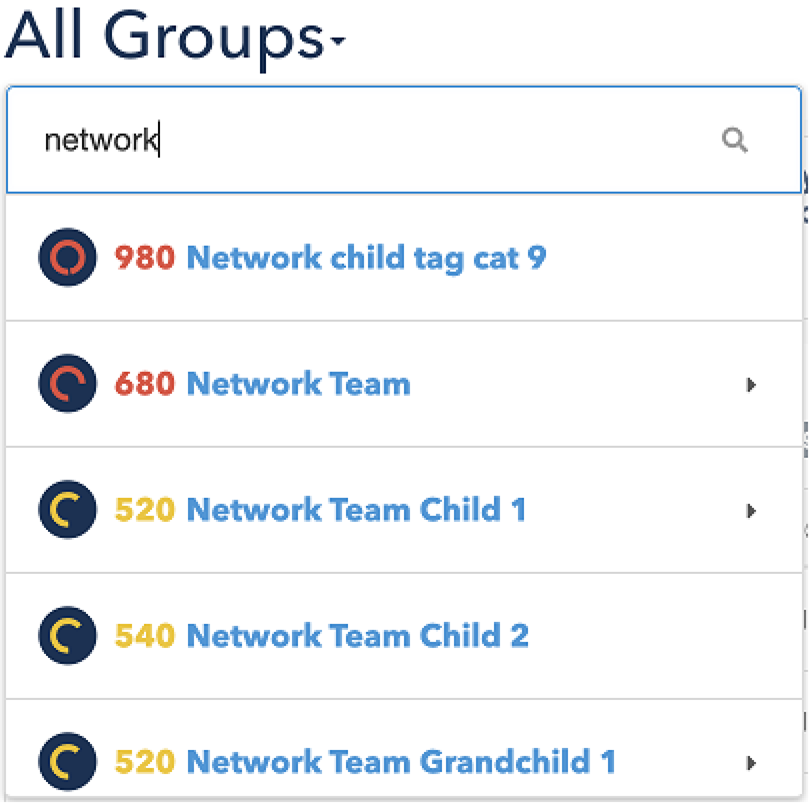
Dashboard Views

★ My Risk Meters

☆ Main Dashboard

Using the VM Explore page

The VM Explore page makes it easy for you to use risk meters, also known as groups, and to search for and filter data. When you first open the Explore page, if you click on All Groups, the first 500 of your organization's groups display in a drop-down list. To find the group that you want to see, start typing in the Search field. Once the group that you want to see displays in the list, click it to view its details.



All Groups

network

980 Network child tag cat 9

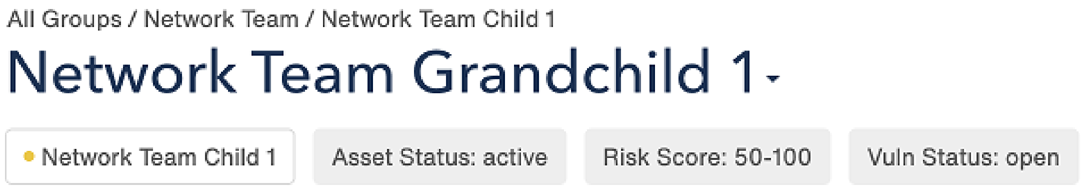
680 Network Team

520 Network Team Child 1

540 Network Team Child 2

520 Network Team Grandchild 1

If you have hierarchical risk meters defined, you can also see their hierarchy in the list. A group that has a hierarchy of groups has an arrow beside its name. Click the arrow and the descendants of the group display. A breadcrumb trail displays above the current group, which is also another way to navigate through your groups. As you examine the child risk meters, the breadcrumb trail shows the path you are taking. You can click on any of the items in the breadcrumb trail to display that group. In the following image, the hierarchy of groups is **All Groups > Network Team > Network Team Child 1 > Network Team Grandchild 1**.



All Groups / Network Team / Network Team Child 1

Network Team Grandchild 1

Network Team Child 1 | Asset Status: active | Risk Score: 50-100 | Vuln Status: open

Using Asset Tags

Metadata about assets are called Tags in Cisco Vulnerability Management. Tags are automatically imported and synchronized with assets during connector runs. Tags can also be added using the UI or API. Tagging assets allows you to maintain a structure that you have already established in your scanner tools. Some common tags include Asset Groups and Tags from Qualys, Sites from Nexpose, Tags from Tenable, and various data fields from ServiceNow CMDB such as Model Number, Location, and Asset Tag. Tags help many customers filter and segregate data to build risk meters.

Vulnerability Statuses

On the VM Explore page. you can modify the status of a vulnerability to help your team prioritize the vulnerabilities that matter and to track the lifecycle of your vulnerabilities. The Cisco Vulnerability Management offers four vulnerability statuses:

- **Open**: The vulnerability is still a risk in your organizational data and is available in Cisco Vulnerability Management for remediation. This is the default status for vulnerabilities.
- **Closed**: The vulnerability has been remediated by your team. Once closed, it is removed from the Open vulnerability view.
- **Risk Accepted**: The vulnerability truly represents a risk, but the business has decided not to remediate it for some reason. A good example of a Risk Accepted vulnerability is an Internet Explorer vulnerability on a server in a data center that is not accessed or Java vulnerabilities that cannot be remediated because a legacy application will not be replaced until the next fiscal year.
- **False Positive**: The vulnerability identified in your scan file is not actually a vulnerability.

Modify the status of a vulnerability

1. Navigate to the VM Explore page.
2. Click the checkbox beside the vulnerability that you want to change the status for.
3. Click **Set Status**.
4. Select a vulnerability status option.

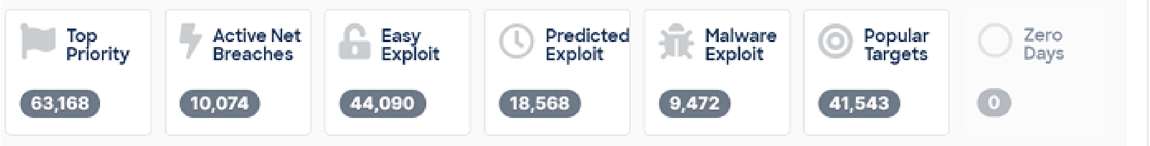
You will see the risk status that you’ve assigned to the vulnerability when you click one of the vulnerabilities in the table and view its details. You can also flag many vulnerabilities at once as either risk accepted or false positive in the Vulnerability table (or all at once using the Display drop-down). Once selected, just assign the new status using the drop-down.

Flagging a vulnerability as risk accepted or as false positive will remove those items from the risk meter score, as only open vulnerabilities contribute to an asset score. For Risk Meters that would have contained vulnerabilities that you marked risk accepted, you will see the Risk Meters True Risk score on the Group Overview of the Reporting page.

You can add additional information to your vulnerability statuses (such as justification of the decision or a date to reevaluate) by creating a custom field for each. For Risk Accepted items, a Due Date is also recommended so that the business can revisit the decision to not remediate the risk. For more information on using custom fields, see the information here.

Filter and search for data

You can use filtering options at the top of the page to help you search for identified vulnerabilities. You can select multiple options to refine the filtered view.



Here is what each of the filters do:

Top Priority: Identifies the highest priority vulnerabilities which will most improve your security posture if they are addressed.

Active Net Breaches: Identifies vulnerabilities that are being successfully exploited in the wild currently.

Easily Exploitable: Identifies vulnerabilities that are included in exploit kits or other public exploit sources.

Predicted Exploitable: Identifies the number of vulnerabilities that are predicted to become exploitable.

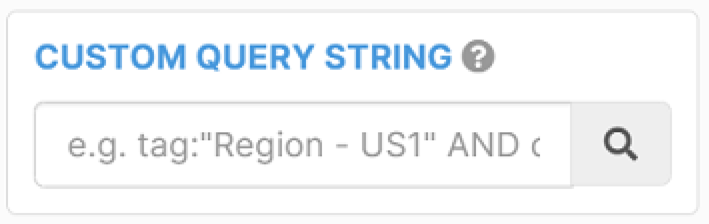
Malware Exploitable: Identifies the number of vulnerabilities actively exploited with Malware including Trojans, Worms, Ransomware, and more.

Popular Targets: Identifies the number of vulnerabilities that other Cisco Vulnerability Management clients are seeing in high volume.

Zero Days: Identifies 0-day vulnerabilities that are recently discovered vulnerabilities (or bugs) that are not yet known to vendors or anti-virus companies, that hackers can exploit.

Custom Query String

In the Custom Query String Search bar, you can search for specific details about Assets, or Vulnerabilities. For example, you can search for an asset by ID: "asset_id:32716281", or a vulnerability by specific CVE identifier: "cve:2014-0160".

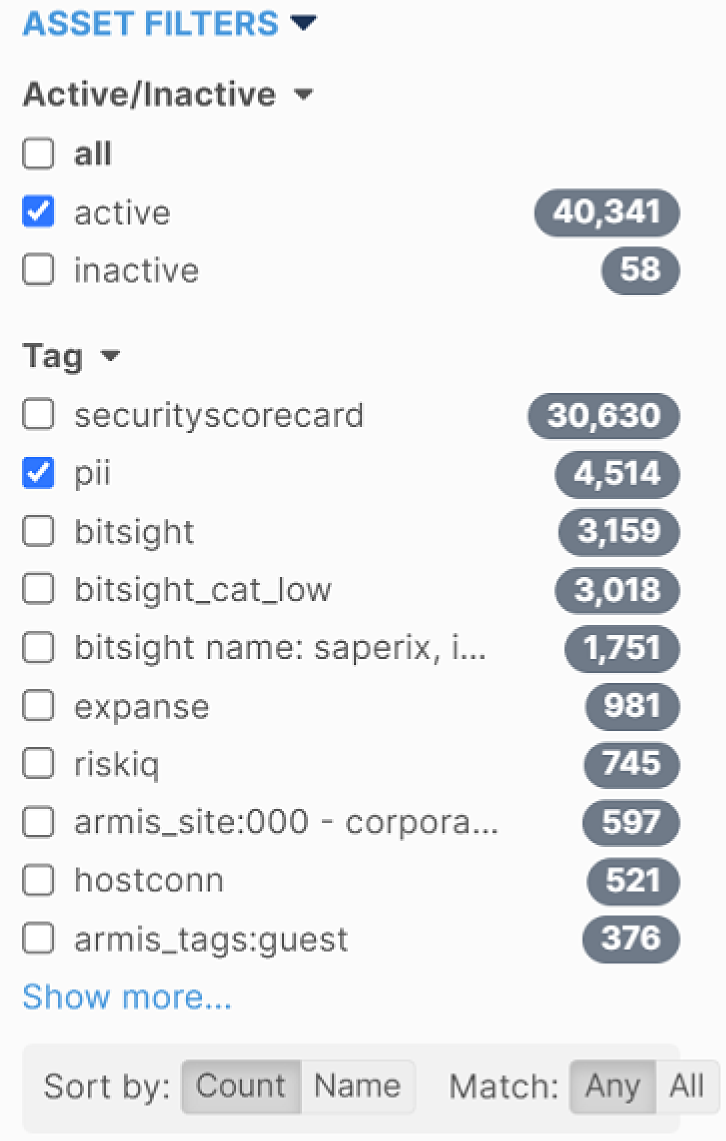


CUSTOM QUERY STRING

e.g. tag:"Region - US1" AND c

Filters section

You can also use the options in the Asset Filters and Vulnerability Filters sections to adjust the list that displays.



ASSET FILTERS

Active/Inactive

□ all	
☑ active	40,341
□ inactive	58

Tag

□ securityscorecard	30,630
☑ pii	4,514
□ bitsight	3,159
□ bitsight_cat_low	3,018
□ bitsight name: saperix, i...	1,751
□ expanse	981
□ riskiq	745
□ armis_site:000 - corpora...	597
□ hostconn	521
□ armis_tags:guest	376

Show more...

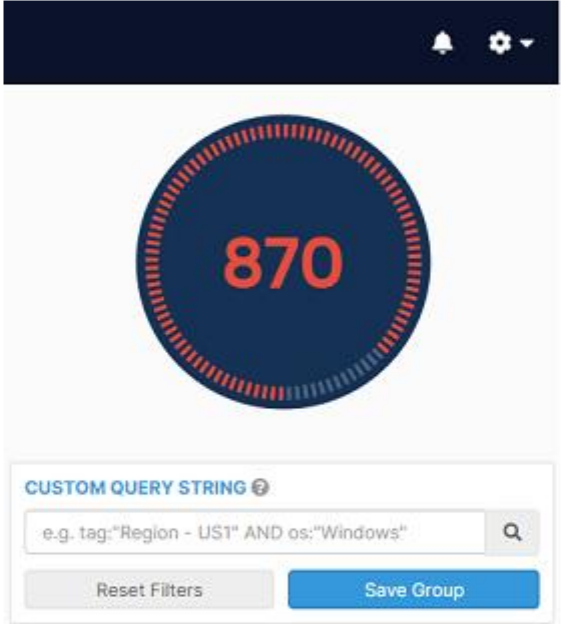
Sort by: [✓ Count] Name Match: [✓ Any] All

Create, Edit, and Delete a Risk Meter

Administrators, normal users, and custom users that have the "Edit Asset Groups" permission assigned to them can create, edit, and delete risk meters.

Create a Risk Meter

1. On the **VM > Explore** page, in the **Custom Query String** field, or using the **Asset Filters** options, perform a search.
2. After you have captured the assets or vulnerabilities that you want, click **Save Group**.

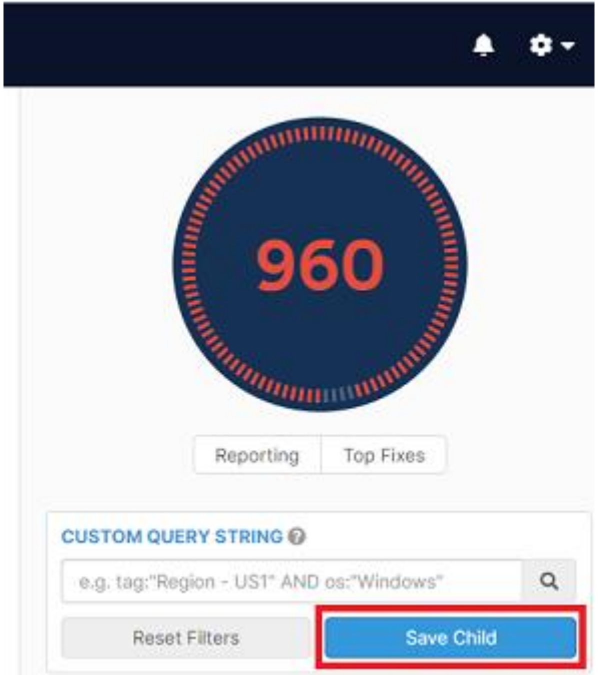


3. In the **Create Group** pop-up window, type a name for the risk meter and choose the roles that can access it.
4. Click **Create Group**.

Create a child risk meter

1. On the **VM > Explore** page, use the search field to find the risk meter that you want to create a child risk meter for, and click it.
2. Hover over the name of the risk meter.
3. Click ⊕.

4. In this Child Risk Meter view, add any additional filters and then click **Save Child**.



5. In the Create Child Group pop-up window, enter a name and select any roles.
6. Click **Create Child**.

Edit a Risk Meter

1. On the **VM > Explore** page, use the search field to find the risk meter that you want to edit, and click it.
2. Hover over the name of the risk meter.
3. Click ✎.
4. Edit the group name, role permissions, or filters.
5. Click **Update Group**.

Delete a Risk Meter

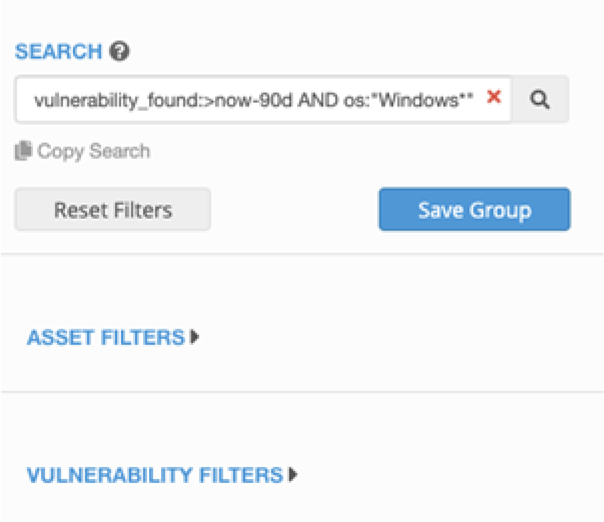
1. On the **VM > Explore** page, use the search field to find the risk meter that you want to delete, and click it.
2. Hover over the name of the risk meter.
3. Click 🗑.
4. In the Confirm Delete Risk Meter pop-up window, click **Yes, Delete**.
   Note: Deleting a risk meter permanently deletes all data from that meter and all its descendants.

Create, Edit, and Delete Risk Meters

A risk meter is simply a saved search, but it provides a lot more benefits, such as Reporting and Top Fixes. Administrators, normal users, and custom users with permission to "Edit Asset Groups" can create, edit, and delete risk meters.

Create a Risk Meter

1. In Cisco Vulnerability Management, click **VM > Explore**.
2. Use the filters to reduce the data that displays in the view.



vulnerability_found:>now-90d AND os:"Windows*"

3. To save your search as a new Risk Meter, click **Save Group**.
4. Name the Risk Meter.
5. Select the Roles that you want assigned to the Risk Meter.
6. Click **Create Group**.

Update a Risk Meter

After you have created a Risk Meter, you can change its name, permissions, or the filters.

1. In Cisco Vulnerability Management, click **VM > Explore**.
2. Hover over the name of the risk meter.
3. Click ✎.
4. Click **Name/Permissions**, or **Filters** depending on what you want to edit.
5. Edit the Risk Meter.
6. Click **Update Group**.

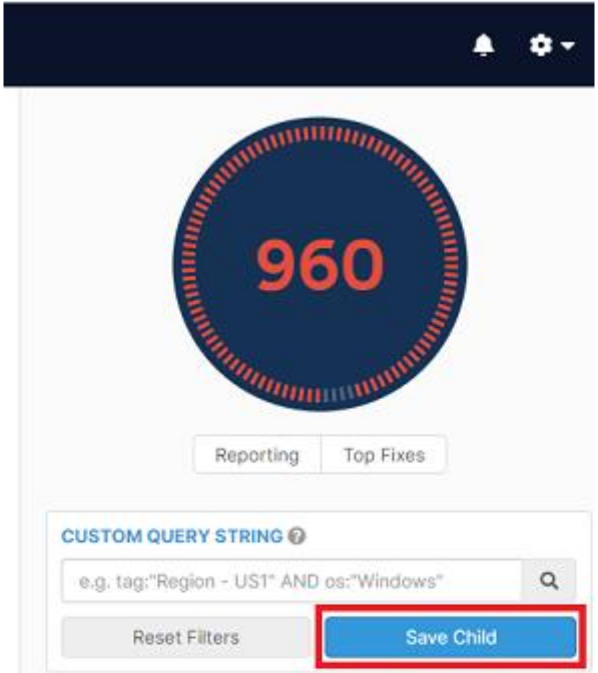
Delete a Risk Meter

Note: Deleting a risk meter permanently deletes all data from that meter and all its descendants.

1. On the VM > Explore page, use the search field to find the risk meter that you want to delete, and click it.
2. Hover over the name of the risk meter.
3. Click 🗑.
4. In the Confirm Delete Risk Meter pop-up window, click **Yes, Delete**.

Create a Child Risk Meter

1. On the **VM > Explore** page, use the search field to find the risk meter that you want to create a child risk meter for, and click it.
2. Hover over the name of the risk meter.
3. Click ⊕.
4. In the Child Risk Meter view, add any additional filters and then click **Save Child**.



5. In the Create Child Group pop-up window, enter a name and select any roles.
6. Click **Create Child**.

Understanding Vulnerability, Asset and Risk Meter Scoring

There are three main components of scoring in Cisco Vulnerability Management. Understanding these scoring concepts for vulnerabilities, assets and risk meters will help you use Cisco Vulnerability Management more effectively.

Component 1: Vulnerability Scoring

In Cisco Vulnerability Management, vulnerabilities from your various scanning vendors are imported during connector runs and normalized based on the CVE ID, CWE ID, or the WASC identifier.

For network vulnerabilities, Cisco Vulnerability Management looks at the CVSS base score for the CVE. It then looks at 20+ threat and exploit feeds to understand the volume and velocity of attacks against that CVE, if there is malware available, if it is easy to exploit, whether it is actively being exploited in the wild, and so on. Cisco Vulnerability Management uses all of these details help calculate the Vulnerability Score.

For application vulnerabilities, scores are based on the Cisco Security Risk Score from the scanner or a base CWE (Common Weakness Enumeration) score if a scanner score is not available.

Vulnerabilities get a score from 0-100 and are broken into thirds:

- Green 0-33
- Amber 34-66
- Red 67-100

Component 2: Asset Scoring

When Cisco Vulnerability Management calculates the score for an asset, it looks at the highest scored vulnerability present on the asset. Cisco Vulnerability Management considers an asset to be as at risk as its highest vulnerability. This is an important concept to understand because the asset score is not an average based on all the vulnerabilities that are present. As you remediate vulnerabilities on an asset, if you remediate vulnerabilities that are not the highest scored vulnerabilities, the asset score will not change.

Assets get a score from 0-1000 and are broken into thirds and rounded to the nearest 10:

- Green 0-330
- Amber 340-660
- Red 670-1000

The way the default asset score is calculated is to look at the highest scored vulnerability and multiply it by the asset priority. Asset priority is set to 10 by default but is adjustable per asset. For more information on asset priority, refer to Asset Prioritization In Cisco Vulnerability Management or discuss with your CX team.

Highest Vuln Score	**X**	**Asset Priority**	**=**	**Default Asset Score**
100	X	10	=	1000
80	X	10	=	800
100	X	7	=	700
70	X	6	=	420

Internal vs External IP Scoring

In addition to the default asset score, Cisco Vulnerability Management also applies a 200 point increase in score if the asset has an External IP Address because external facing assets represent a higher risk. Cisco Vulnerability Management, by default, considers any asset with an IP other than a 10.*, 172.16.0.0 -172.31.255.255 and 192.168.* to be an external asset. The highest score will still be 1000 for assets.

Note: This external 200 point increase can be disabled for those customers who use publicly routable IP space internally. For more information, contact your CX team member .

Highest Vuln Score	**X**	**Asset Priority**	**=**	**Default Asset Score**	**External IP?**	**+**	**Final Asset Score**
100	X	10	=	1000	yes	200	1000
80	X	10	=	800	no	0	800
100	X	7	=	700	yes	200	900
70	X	6	=	420	yes	200	620

Component 3: Risk Meter Score

The last component of scoring is the Risk Meter Score. This score is calculated by taking the average of all of the active, non-zero scored assets in the group. Risk Meters are assigned a score between 0-1000 and are broken into thirds and rounded to the nearest 10:

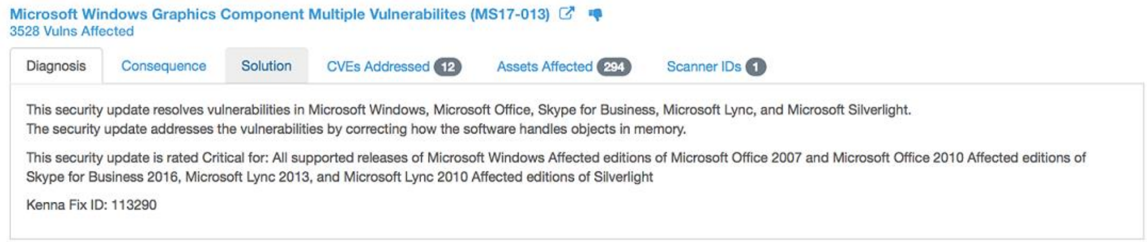
- Green 0-330
- Amber 340-660
- Red 670-1000

Fixes and Top Fix Groups

You can manage individual fixes or fix groups.

Fixes

The fixes view on the VM Explore page will show all available fixes for the vulnerabilities and assets that are being displayed. Fixes are sorted by the number of associated vulnerabilities:



Microsoft Windows Graphics Component Multiple Vulnerabilites (MS17-013)
3528 Vulns Affected

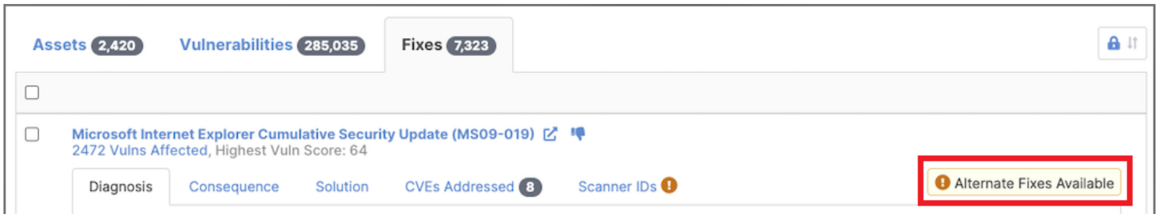
This security update resolves vulnerabilities in Microsoft Windows, Microsoft Office, Skype for Business, Microsoft Lync, and Microsoft Silverlight.
The security update addresses the vulnerabilities by correcting how the software handles objects in memory.

This security update is rated Critical for: All supported releases of Microsoft Windows Affected editions of Microsoft Office 2007 and Microsoft Office 2010 Affected editions of Skype for Business 2016, Microsoft Lync 2013, and Microsoft Lync 2010 Affected editions of Silverlight

Kenna Fix ID: 113290

Each Fix displays all of the related CVEs and each of the assets that those CVEs affect. Cisco Vulnerability Management also includes a diagnosis (a brief description of the vulnerability), the consequence (what a successful exploit could result in or allow an attacker to do), and solutions (how, specifically, to remediate the vulnerability), based on vendor data.
Users can filter by Cisco Security Risk Score and threat vectors to display the highest risk items and view the number of assets and vulnerabilities that would be involved in the remediation.

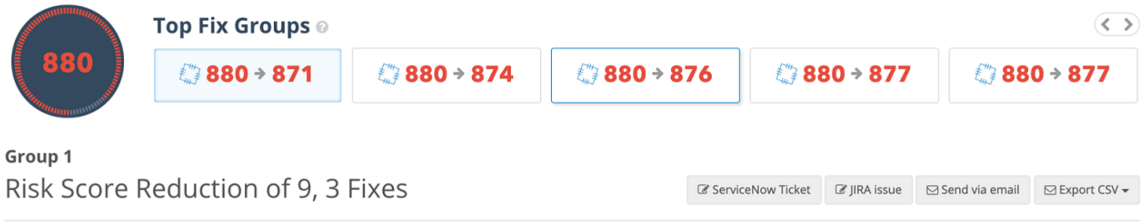
Note: If there are more fixes available for the fix that you are viewing, an Alternate Fixes Available button displays. When you click the button a list of links to alternate fixes displays. You can click the links to see more information about the fixes.



Microsoft Internet Explorer Cumulative Security Update (MS09-019)
2472 Vulns Affected, Highest Vuln Score: 64

Top Fixes

For each risk group, Cisco Vulnerability Management provides Top Fixes. To access the top fixes, on the VM Dashboard page, navigate to the risk meter that you want to see the top fixes for and click the Top Fixes button. Each Top Fix is a group of up to 3 fixes that fall in the top 10 largest risk reductions for that Risk Meter. The Top Fix view for a Risk Meter contains its current Cisco Security Risk Score, along with the lower score that the Risk Meter would move to after remediating all vulnerabilities in a specific Fix Group. These are sorted by largest risk reduction, left to right, with a button on the right side to move to the second page of Top Fixes.



Group 1

Risk Score Reduction of 9, 3 Fixes

In the example above, remediating the vulnerabilities for all 3 listed Fixes will reduce the current Cisco Security Risk Score of 880 by 9 points, down to a new score of 871.

All of the Top Fix Groups (not just the one currently displayed) can be exported in this view by clicking the "Export CSV" button or you can also create a ticket to send out the fix information to the remediation owner (if you have a ticketing connector set up).

Top Fixes Best Practices

Top Fixes are valuable for quickly reducing overall risk. They are based on a pretty simple mathematical calculation that looks at the possible risk reduction to the average risk meter score achieved through applying up to 3 fixes. The calculation depends on two things:

1. There are a good number of assets that have the same vulnerabilities in the Risk Meter.
2. A score reduction can be found with three or less fixes applied.

Top Fixes is good for:

- Providing remediation teams a place to focus efforts, particularly early on, and achieve quick wins in risk reduction.
- Grouping fixes together in a way that will achieve the biggest risk reduction for the remediation efforts.

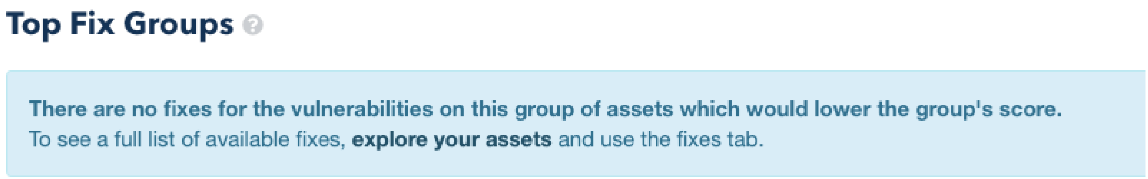
Top Fixes is not good for:

- Remediating "legacy" devices with lots of vulnerabilities.
- Risk Meters with dissimilar machines and operating systems.
- Finding quick wins when there are more than three vulnerabilities at the same score level on many of the assets.

As customers mature and take care of the highest-level vulnerabilities, top fixes become less and less useful because most vulnerabilities in Cisco Vulnerability Management are scored in the 30-40 range. Therefore, when a customer has most assets remediated to reflect a lower score, Top Fixes will find fewer and fewer recommended fixes. In addition to using Top Fixes, Cisco recommends that Cisco Vulnerability Management administrator teams train their staff to look at vulnerabilities by Cisco Security Risk Score from the Explore view, and remediate any vulnerabilities that are out of risk appetite.

Why are there no Top Fixes?

When no individual fixes would change the overall score of a Risk Meter, no "Top Fixes" are populated. When this happens, the following message displays: "There are no fixes for the vulnerabilities in this group of assets which would lower the group's score."



Top Fix Groups

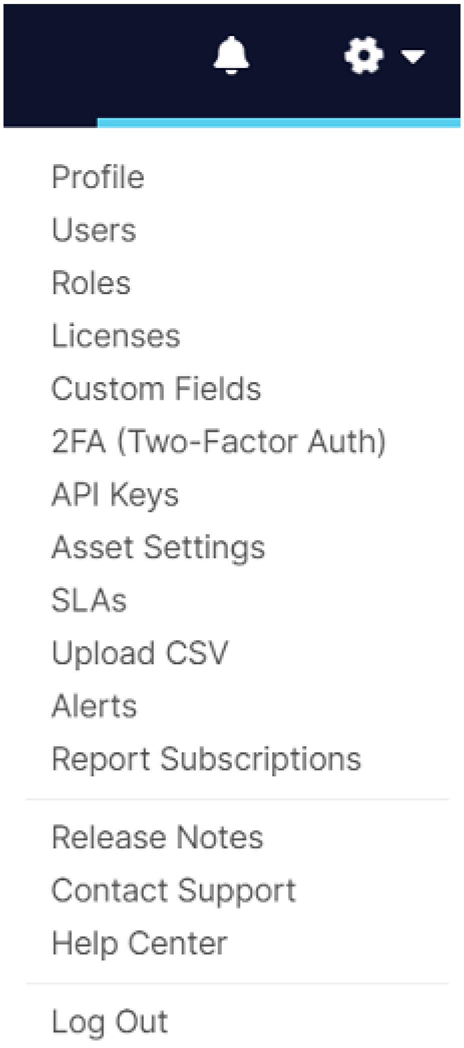
There are no fixes for the vulnerabilities on this group of assets which would lower the group's score.
To see a full list of available fixes, **explore your assets** and use the fixes tab.

There are many reasons why you might not see any top fixes, but here are some examples:

- If your risk meter is vulnerability-based, and none of the vulnerabilities contained in the risk meter are the highest vulnerability on the asset, there will be no opportunity for risk reduction because the vulnerabilities that would affect the score were excluded. Risk Meter scores are an average of asset scores and assets are only scored on the highest vulnerability on the asset.
- If you have a vulnerability-based risk meter focusing only on vulnerabilities scored at 100, even if you remediate those highest-scored vulnerabilities on the assets, the remaining vulnerabilities will still result in a risk meter score of 1000.
- If all assets in the risk meter have so many high scored vulnerabilities on them that it would take more than 3 fixes to achieve a risk reduction, no fixes will be displayed. Cisco Vulnerability Management shows you fix groups that contain up to three fixes only so as to provide manageable achievable risk reductions. In this scenario, go to the Explore page for the risk meter, sort or filter on the highest vulnerabilities, and then look at the associated fixes.
- If your risk meter has no data, contains only inactive assets, or only contains assets scored at 0, the risk meter score will always be 0 and no top fixes will change that.

Using the Settings menu

You can use the Settings menu to perform numerous functions.



Description of Settings menu items

Menu item	**Description**
Profile	View and edit your profile such as email address, and setting a new password.
Users	View, edit, and add Cisco Vulnerability Management users.
Roles	View, edit, and add Cisco Vulnerability Management roles.
Licenses	View how many of your licenses are being used out of the total purchased. An exclamation point means you have exceeded the number of licenses that you have

	purchased. This page also displays the Organization ID that Cisco uses as a company identifier.
Custom Fields	View, edit, delete, and create custom fields for VM and Application Security Module.
2FA (Two-Factor Auth)	Used to set up Two-Factor Authentication for your organization.
API Keys	View who has an API key assigned to them, generate a new token for a user, or remove their API Key. API Keys give access to your users to access the API.
Asset Settings	Used to set asset inactivity limits, and the asset purge period.
SLAs	Used to set up risk based Service Level Agreements SLAs. An SLA is a time-based requirement in which a vulnerability must be fixed.
Upload CSV	Used to import assets or metadata on assets from a CSV file.
Alerts	Create and maintain in-app and email alerts. For example, you can chose to receive an alert when a group score changes or when new active internet breaches are identified.
Report Subscriptions	View, edit, delete, and create report subscriptions so that you can see specific configured Risk Meter reports.
Release Notes	View the latest release notes document.
Contact Support	Search for help topics or contact support.
Help Center	View the Cisco Vulnerability Management documentation.
Log Out	Log out of Cisco Vulnerability Management.