



# Tenable Exposure Management User Guide

Last Revised: August 28, 2025



# Table of Contents

<b>Welcome to Tenable Exposure Management</b>	<b>36</b>
Get Started with Tenable Exposure Management	37
Configure your "Point Products" to get Data into Tenable Exposure Management	38
License, Access, and Log In	40
Configure Tenable Exposure Management for Use	40
Analyze and Assess	40
Tenable Exposure Management Use Cases	43
Licensing	45
Licensing Tenable One	45
Tenable One Components	46
Tenable One Asset Values	47
Reclaiming Licenses	48
Exceeding the License Limit	48
Expired Licenses	48
Tenable Exposure Management System Requirements	49
Key Terms	49
Data Sources	53
Data Timing	56
Tenable Exposure Management Metrics	56
Data Timing	56
Cyber Exposure Score (CES)	57
Asset Exposure Score (AES)	57
Asset Criticality Rating (ACR)	57



Vulnerability Priority Rating (VPR) .....	58
Exposure Categories .....	58
Scoring Caveats within Tenable Exposure Management .....	59
Log in to Tenable Exposure Management .....	60
Navigate Tenable Exposure Management .....	60
Log out of Tenable Exposure Management .....	68
<b>Home .....</b>	<b>69</b>
<b>Exposure Signals .....</b>	<b>81</b>
Manage Exposure Signals .....	91
<b>Inventory .....</b>	<b>102</b>
Assets .....	103
Asset Classes .....	111
Asset Filters .....	112
Global Asset Search .....	119
NLP Search Use Cases .....	129
Asset Details .....	130
Tag Assets via the Assets Page .....	160
Weaknesses .....	162
Weakness Details .....	169
Findings .....	173
Finding Details .....	180
Software .....	183
Software Details .....	190
Dashboards .....	193



Dashboard Overview .....	197
Manage Dashboards .....	201
Valid Custom Widget Combinations .....	212
Exposure View .....	216
Manage the Exposure View Page .....	235
Manage Exposure Cards .....	246
<b>Attack Path .....</b>	<b>257</b>
Dashboard .....	260
Top Attack Paths .....	262
Generate an Attack Path Query with the Attack Path Query Builder .....	267
(Optional) Save your Query as a Preset/Bookmark .....	271
Generate an Asset Exposure Query .....	271
Generate a Blast Radius Query .....	274
Interact with Attack Path Query Data .....	276
Generate an Asset Query with the Asset Query Builder .....	285
Interact with Asset Query Data .....	287
Generate an Attack Path with a Built-in Query .....	293
Query Types in the Query Library .....	296
Supported Attack Path Techniques .....	300
Top Attack Techniques .....	300
Attack Technique Details .....	306
Manage Attack Techniques .....	311
MITRE ATT&CK Heatmap .....	316
<b>Tags .....</b>	<b>320</b>





Tag Format and Application .....	323
Tag Details .....	324
Manage Tags .....	326
<b>Connectors .....</b>	<b>335</b>
What is a Connector .....	335
Why Integrate .....	335
Supported Integrations (Connectors) .....	335
Ingested Data .....	336
View and Manage your Connectors .....	336
Connector Data Status .....	337
Connector Logs .....	340
Access Connector Logs .....	341
Reading Connector Logs .....	342
Log Time Stamp .....	343
Activity (Sync) Type .....	343
Data Stage (Sync Status) .....	344
Data Lifecycle Stages .....	345
Connector Error Messages .....	348
Manage Connectors .....	351
Supported Third-Party Integrations .....	361
Security Tools Supported Integrations .....	361
Asset Inventory Supported Integrations .....	363
Bug Bounty Supported Integrations .....	364
Other Integrations .....	364



Acunetix360 Connector .....	364
Connector Details .....	365
Prerequisites and User Permissions .....	365
Add a Connector .....	366
Configure the Connector .....	367
Acunetix 360 in Tenable Exposure Management .....	369
Locate Connector Assets in Tenable Exposure Management .....	369
Locate Connector Weaknesses in Tenable Exposure Management .....	370
Locate Connector Findings in Tenable Exposure Management .....	371
Data Mapping .....	373
Web Application Mapping .....	373
Finding Mapping .....	373
Finding Status Mapping .....	374
Finding Severity Mapping .....	375
Status Update Mechanisms .....	375
Uniqueness Criteria .....	376
API Endpoints in Use .....	376
Acunetix Premium Cloud Connector .....	376
Connector Details .....	377
Prerequisites and User Permissions .....	377
Add a Connector .....	378
Configure the Connector .....	379
Acunetix Premium in Tenable Exposure Management .....	381
Locate Connector Assets in Tenable Exposure Management .....	381



Locate Connector Weaknesses in Tenable Exposure Management .....	382
Locate Connector Findings in Tenable Exposure Management .....	383
Data Mapping .....	385
Web Application Mapping .....	385
Finding Mapping .....	385
Finding Status Mapping .....	386
Finding Severity Mapping .....	386
API Endpoints in Use .....	387
Armis Connector .....	387
Connector Details .....	387
Prerequisites and User Permissions .....	388
Add a Connector .....	391
Configure the Connector .....	392
Armis in Tenable Exposure Management .....	394
Locate Connector Assets in Tenable Exposure Management .....	394
Locate Connector Findings in Tenable Exposure Management .....	395
Data Mapping .....	396
Device Mapping .....	397
Finding Mapping .....	398
Finding Severity Mapping .....	399
Finding Status Mapping .....	400
Status Update Mechanisms .....	400
Uniqueness Criteria .....	401
Support and Expected Behavior .....	401



API Endpoints in Use .....	402
Data Validation .....	402
Asset Data Validation .....	402
Finding Data Validation .....	405
AWS EC2 Connector .....	407
Connector Details .....	408
Prerequisites and User Permissions .....	408
Add a Connector .....	412
Configure the Connector .....	413
AWS in Tenable Exposure Management .....	415
Locate Connector Assets in Tenable Exposure Management .....	415
Data Mapping .....	416
Device Mapping .....	416
Resource Mapping .....	417
Status Update Mechanisms .....	418
Support Limitations and Expected Behavior .....	419
API Endpoints in Use .....	419
Data Validation .....	419
Asset Data Validation .....	419
Security Groups (Resources) Data Validation .....	420
AWS Inspector V2 Connector .....	421
Connector Details .....	421
Prerequisites and User Permissions .....	422
Add a Connector .....	425



Configure the Connector .....	427
AWS in Tenable Exposure Management .....	428
Locate Connector Assets in Tenable Exposure Management .....	428
Locate Connector Weaknesses in Tenable Exposure Management .....	429
Locate Connector Findings in Tenable Exposure Management .....	430
Data Mapping .....	432
Device Mapping .....	432
Container Mapping .....	432
Resource Mapping .....	433
Finding Mapping .....	433
Finding Status Mapping .....	434
Finding Severity Mapping .....	434
Status Update Mechanisms .....	435
Uniqueness Criteria .....	436
API Endpoints in Use .....	436
Data Validation .....	436
Asset Data Validation .....	437
Finding Data Validation .....	438
Axonius Connector .....	439
Connector Details .....	439
Prerequisites and User Permissions .....	440
Add a Connector .....	441
Configure the Connector .....	442
Axonius in Tenable Exposure Management .....	444



Locate Connector Assets in Tenable Exposure Management .....	444
Data Mapping .....	445
Device Mapping .....	445
Uniqueness Criteria .....	447
API Endpoints in Use .....	447
Support Limitations and Expected Behavior .....	448
Data Validation .....	448
Asset Data Validation .....	448
Azure Connector .....	449
Connector Details .....	450
Prerequisites and User Permissions .....	450
Add a Connector .....	452
Configure the Connector .....	453
Azure in Tenable Exposure Management .....	456
Locate Connector Assets in Tenable Exposure Management .....	456
Data Mapping .....	457
Device Mapping .....	458
Status Update Mechanisms .....	459
Uniqueness Criteria .....	459
API Endpoints in Use .....	460
Data Validation .....	461
Asset Data Validation .....	461
BitSight Connector .....	462
Connector Details .....	462



Prerequisites and User Permissions .....	463
Add a Connector .....	463
Configure the Connector .....	465
BitSight in Tenable Exposure Management .....	466
Locate Connector Assets in Tenable Exposure Management .....	467
Locate Connector Weaknesses in Tenable Exposure Management .....	468
Locate Connector Findings in Tenable Exposure Management .....	469
Data Mapping .....	471
Device Mapping .....	471
Device Finding Mapping .....	471
Web Application Mapping .....	472
Web Application Finding Mapping .....	472
Finding Status Mapping .....	473
Finding Severity Mapping .....	473
Status Update Mechanisms .....	474
Uniqueness Criteria .....	474
API Endpoints in Use .....	475
Data Validation .....	475
Asset Data Validation .....	475
Finding Data Validation .....	476
BlackDuck (formerly WhiteHat) Connector .....	477
Connector Details .....	477
Prerequisites and User Permissions .....	478
Add a Connector .....	478



Configure the Connector .....	480
BlackDuck Continuous Dynamic in Tenable Exposure Management .....	481
Locate Connector Assets in Tenable Exposure Management .....	481
Locate Connector Weaknesses in Tenable Exposure Management .....	482
Locate Connector Findings in Tenable Exposure Management .....	483
Data Mapping .....	485
Web Application Mapping .....	485
Finding Mapping .....	486
Finding Status Mapping .....	486
Finding Severity Mapping .....	487
Uniqueness Criteria .....	487
Status Update Mechanisms .....	488
API Endpoints in Use .....	488
Data Validation .....	489
Asset Data Validation .....	489
Finding Data Validation .....	490
Cortex XDR Connector .....	491
Connector Details .....	491
Prerequisites and User Permissions .....	492
Add a Connector .....	492
Configure the Connector .....	493
Locate Connector Assets in Tenable Exposure Management .....	495
Locate Connector Weaknesses in Tenable Exposure Management .....	496
Locate Connector Findings in Tenable Exposure Management .....	497





Data Mapping .....	499
Device Mapping .....	499
Finding Mapping .....	499
Finding Severity Mapping .....	500
Finding Status Mapping .....	500
Status Update Mechanisms .....	500
Uniqueness Criteria .....	501
API Endpoints in Use .....	501
Support Limitations and Expected Behavior .....	502
Data Validation .....	502
Asset Data Validation .....	502
Finding Data Validation .....	503
CrowdStrike Connector .....	505
Connector Details .....	505
Prerequisites and User Permissions .....	505
Add a Connector .....	506
Configure the Connector .....	507
Crowdstrike in Tenable Exposure Management .....	509
Locate Connector Assets in Tenable Exposure Management .....	509
Locate Connector Weaknesses in Tenable Exposure Management .....	511
Locate Connector Findings in Tenable Exposure Management .....	512
Data Mapping .....	513
Device Mapping .....	514
Finding Mapping .....	515



Finding Severity Mapping .....	515
Finding Status Mapping .....	516
Status Update Mechanisms .....	516
Uniqueness Criteria .....	517
API Endpoints in Use .....	517
Data Validation .....	518
Asset Data Validation .....	518
Finding Data Validation .....	519
CyCognito Connector .....	520
Connector Details .....	521
Prerequisites and User Permissions .....	521
Add a Connector .....	522
Configure the Connector .....	523
CyCognito in Tenable Exposure Management .....	525
Locate Connector Assets in Tenable Exposure Management .....	525
Locate Connector Weaknesses in Tenable Exposure Management .....	526
Locate Connector Findings in Tenable Exposure Management .....	527
Data Mapping .....	529
Device Mapping (CyCognito IP Address) .....	529
Web Application Mapping (CyCognito Web Applications) .....	530
Web Application Mapping (CyCognito Domain) .....	531
Finding Mapping .....	532
Finding Status Mapping .....	533
Finding Severity Mapping .....	533



Status Update Mechanisms .....	533
Uniqueness Criteria .....	534
Support Limitations and Expected Behavior .....	535
API Endpoints in Use .....	536
Data Validation .....	536
Asset Data Validation .....	537
Finding Data Validation .....	539
Detectify Connector .....	540
Connector Details .....	541
Prerequisites and User Permissions .....	541
Add a Connector .....	542
Configure the Connector .....	543
Detectify in Tenable Exposure Management .....	545
Locate Connector Assets in Tenable Exposure Management .....	545
Locate Connector Weaknesses in Tenable Exposure Management .....	546
Locate Connector Findings in Tenable Exposure Management .....	547
Data Mapping .....	549
Web Application Mapping .....	549
Finding Mapping .....	549
Finding Status Mapping .....	550
Finding Severity Mapping .....	551
Status Update Mechanisms .....	551
Uniqueness Criteria .....	552
API Endpoints in Use .....	552



Data Validation .....	553
Asset Data Validation .....	553
Finding Data Validation .....	554
HackerOne Connector .....	557
Connector Details .....	557
Prerequisites and User Permissions .....	558
Add a Connector .....	558
Configure the Connector .....	559
HackerOne in Tenable Exposure Management .....	561
Locate Connector Assets in Tenable Exposure Management .....	561
Locate Connector Weaknesses in Tenable Exposure Management .....	562
Locate Connector Findings in Tenable Exposure Management .....	563
Data Mapping .....	565
Web Application Mapping .....	565
Finding Mapping .....	565
Finding Status Mapping .....	567
Finding Severity Mapping .....	567
Status Update Mechanisms .....	568
Uniqueness Criteria .....	568
Support Limitations and Expected Behavior .....	569
API Endpoints in Use .....	569
Data Validation .....	570
Asset Data Validation .....	570
Finding Data Validation .....	571



Intune Connector .....	573
Connector Details .....	573
Prerequisites and User Permissions .....	574
Add a Connector .....	577
Configure the Connector .....	578
Locate Connector Assets in Tenable Exposure Management .....	580
Data Mapping .....	581
Device Mapping .....	581
Uniqueness Criteria .....	583
API Endpoints in Use .....	583
Support Limitations and Expected Behavior .....	583
Data Validation .....	584
Asset Data Validation .....	584
Jamf Pro Connector .....	585
Connector Details .....	585
Prerequisites and User Permissions .....	585
Add a Connector .....	586
Configure the Connector .....	587
Jamf Pro in Tenable Exposure Management .....	589
Locate Connector Assets in Tenable Exposure Management .....	589
Data Mapping .....	590
Device Mapping .....	590
Status Update Mechanisms .....	592
Uniqueness Criteria .....	592



API Endpoints in Use .....	592
Data Validation .....	593
Asset Data Validation .....	593
Microsoft TVM Connector .....	594
Connector Details .....	594
Prerequisites and User Permissions .....	595
Add a Connector .....	597
Configure the Connector .....	598
Microsoft TVM in Tenable Exposure Management .....	600
Locate Connector Assets in Tenable Exposure Management .....	600
Locate Connector Weaknesses in Tenable Exposure Management .....	601
Locate Connector Findings in Tenable Exposure Management .....	602
Data Mapping .....	604
Device Mapping .....	604
Finding Mapping .....	605
Finding Status Mapping .....	606
Finding Severity Mapping .....	606
Status Update Mechanisms .....	607
Uniqueness Criteria .....	607
API Endpoints in Use .....	608
Data Validation .....	608
Asset Data Validation .....	609
Finding Data Validation .....	612
Outpost24 Connector .....	613



Connector Details .....	614
Prerequisites and User Permissions .....	614
Add a Connector .....	621
Configure the Connector .....	622
Outpost 24 in Tenable Exposure Management .....	624
Locate Connector Assets in Tenable Exposure Management .....	624
Locate Connector Weaknesses in Tenable Exposure Management .....	625
Locate Connector Findings in Tenable Exposure Management .....	626
Data Mapping .....	628
Device Mapping .....	628
Finding Mapping (for Device) .....	628
Web Application Mapping .....	629
Finding Mapping (for Web Application) .....	630
Finding Status Mapping .....	631
Finding Severity Mapping .....	631
Status Update Mechanisms .....	632
Uniqueness Criteria .....	633
Support Limitations and Expected Behavior .....	633
API Endpoints in Use .....	634
Data Validation .....	635
Asset Data Validation .....	635
Finding Data Validation .....	636
PrismaCloud CWPP Connector .....	637
Connector Details .....	638



Prerequisites and User Permissions .....	638
Add a Connector .....	640
Configure the Connector .....	641
Prisma CWPP in Tenable Exposure Management .....	643
Locate Connector Assets in Tenable Exposure Management .....	643
Locate Connector Weaknesses in Tenable Exposure Management .....	644
Locate Connector Findings in Tenable Exposure Management .....	645
Data Mapping .....	647
Device Mapping .....	647
Finding Mapping (for Devices) .....	647
Container Mapping .....	648
Finding Mapping (for Containers) .....	649
Finding Status Mapping .....	650
Finding Severity Mapping .....	650
Status Update Mechanisms .....	650
Uniqueness Criteria .....	651
API Endpoints in Use .....	651
Purplemet Connector .....	652
Connector Details .....	652
Prerequisites and User Permissions .....	652
Add a Connector .....	653
Configure the Connector .....	654
Purplemet in Tenable Exposure Management .....	656
Locate Connector Assets in Tenable Exposure Management .....	656





Locate Connector Weaknesses in Tenable Exposure Management .....	657
Locate Connector Findings in Tenable Exposure Management .....	658
Data Mapping .....	660
Web Application Mapping .....	660
Finding Mapping .....	660
Finding Status Mapping .....	661
Finding Severity Mapping .....	662
Status Update Mechanisms .....	662
Uniqueness Criteria .....	662
API Endpoints in Use .....	663
Data Validation .....	663
Asset Data Validation .....	663
Finding Data Validation .....	664
Qualys Connector .....	666
Connector Details .....	666
Prerequisites and User Permissions .....	666
Add a Connector .....	669
Configure the Connector .....	670
Qualys in Tenable Exposure Management .....	673
Locate Connector Assets in Tenable Exposure Management .....	673
Locate Connector Weaknesses in Tenable Exposure Management .....	674
Locate Connector Findings in Tenable Exposure Management .....	676
Device Mapping .....	677
Finding Mapping .....	679



Finding Status Mapping .....	680
Finding Severity Mapping .....	680
Status Update Mechanisms .....	680
Uniqueness Criteria .....	681
API Endpoints in Use .....	681
Support Limitations and Expected Behavior .....	684
Data Validation .....	685
Asset Data Validation .....	685
Findings Data Validation .....	687
Qualys WAS Connector .....	689
Connector Details .....	689
Prerequisites and User Permissions .....	689
Add a Connector .....	692
Configure the Connector .....	694
Qualys WAS in Tenable Exposure Management .....	695
Locate Connector Assets in Tenable Exposure Management .....	695
Locate Connector Weaknesses in Tenable Exposure Management .....	696
Locate Connector Findings in Tenable Exposure Management .....	698
Data Mapping .....	699
Web Application Mapping .....	699
Finding Mapping .....	700
Finding Status Mapping .....	701
Finding Severity Mapping .....	701
Status Update Mechanisms .....	702



API Endpoints in Use .....	702
Data Validation .....	702
Asset Data Validation .....	703
Finding Data Validation .....	704
Rapid7 Insight AppSec Connector .....	705
Connector Details .....	705
Prerequisites and User Permissions .....	706
Add a Connector .....	706
Configure the Connector .....	707
Rapid7 Insight AppSec in Tenable Exposure Management .....	709
Locate Connector Assets in Tenable Exposure Management .....	709
Locate Connector Weaknesses in Tenable Exposure Management .....	710
Locate Connector Findings in Tenable Exposure Management .....	711
Data Mapping .....	713
Web Application Mapping .....	713
Finding Mapping .....	713
Finding Status Mapping .....	714
Finding Severity Mapping .....	714
Status Update Mechanisms .....	715
Uniqueness Criteria .....	715
API Endpoints in Use .....	716
Rapid7 Insight VM (On-Prem) Connector .....	716
Connector Details .....	716
Prerequisites and User Permissions .....	717



Add a Connector .....	724
Configure the Rapid7 Insight VM Connector .....	725
Rapid7 Insight VM in Tenable Exposure Management .....	727
Locate Connector Assets in Tenable Exposure Management .....	727
Locate Connector Weaknesses in Tenable Exposure Management .....	728
Locate Connector Findings in Tenable Exposure Management .....	729
Data Mapping .....	731
Device Mapping .....	731
Finding Mapping .....	732
Finding Status Mapping .....	732
Finding Severity Mapping .....	733
Status Update Mechanisms .....	733
Uniqueness Criteria .....	734
API Endpoints in Use .....	734
Support Limitations and Expected Behavior .....	735
Data Validation .....	737
Asset Data Validation .....	737
Finding Data Validation .....	738
Rapid7 InsightVM Cloud Connector .....	741
Connector Details .....	741
Prerequisites and User Permissions .....	741
Add a Connector .....	744
Configure the Rapid7 Insight VM Cloud Connector .....	745
Rapid7 Insight VM Cloud in Tenable Exposure Management .....	747



Locate Connector Assets in Tenable Exposure Management .....	747
Locate Connector Weaknesses in Tenable Exposure Management .....	748
Locate Connector Findings in Tenable Exposure Management .....	749
Data Mapping .....	751
Device Mapping .....	751
Finding Mapping .....	751
Finding Status Mapping .....	753
Finding Severity Mapping .....	753
Status Update Mechanisms .....	754
Uniqueness Criteria .....	754
API Endpoints in Use .....	755
Data Validation .....	755
Asset Data Validation .....	755
Finding Data Validation .....	757
RedHat Insights Connector .....	760
Connector Details .....	760
Prerequisites and User Permissions .....	760
Add a Connector .....	762
Configure the Connector .....	763
Red Hat Insights in Tenable Exposure Management .....	765
Locate Connector Assets in Tenable Exposure Management .....	765
Locate Connector Weaknesses in Tenable Exposure Management .....	766
Locate Connector Findings in Tenable Exposure Management .....	767
Data Mapping .....	769



Device Mapping .....	769
Finding Mapping .....	770
Finding Status Mapping .....	770
Finding Severity Mapping .....	771
Status Update Mechanisms .....	771
API Endpoints in Use .....	772
Data Validation .....	772
Asset Data Validation .....	773
Finding Data Validation .....	773
RiskRecon Connector .....	776
Connector Details .....	776
Prerequisites and User Permissions .....	777
Add a Connector .....	777
Configure the Connector .....	778
RiskRecon in Tenable Exposure Management .....	780
Locate Connector Assets in Tenable Exposure Management .....	780
Locate Connector Weaknesses in Tenable Exposure Management .....	781
Locate Connector Findings in Tenable Exposure Management .....	782
Data Mapping .....	784
Web Application Mapping .....	784
Finding Mapping .....	785
Finding Status Mapping .....	785
Finding Severity Mapping .....	786
Status Update Mechanisms .....	786



Uniqueness Criteria .....	787
API Endpoints in Use .....	787
Support Limitations and Expected Behavior .....	787
Data Validation .....	791
Asset Data Validation .....	791
Finding Data Validation .....	792
SecurityScorecard Connector .....	793
Connector Details .....	793
Prerequisites and User Permissions .....	794
Add a Connector .....	794
Configure the Connector .....	795
SecurityScorecard in Tenable Exposure Management .....	797
Locate Connector Assets in Tenable Exposure Management .....	797
Locate Connector Weaknesses in Tenable Exposure Management .....	798
Locate Connector Findings in Tenable Exposure Management .....	799
Data Mapping .....	801
Web Application Mapping .....	801
Finding Mapping .....	801
Finding Status Mapping .....	802
Finding Severity Mapping .....	802
Status Update Mechanisms .....	803
Uniqueness Criteria .....	803
API Endpoints in Use .....	804
Support Limitations and Expected Behavior .....	805



Data Validation .....	805
Asset Data Validation .....	805
Finding Data Validation .....	808
SentinelOne Connector .....	811
Connector Details .....	811
Prerequisites and User Permissions .....	812
Add a Connector .....	813
Configure the Connector .....	814
SentinelOne in Tenable Exposure Management .....	816
Locate Connector Assets in Tenable Exposure Management .....	816
Locate Connector Weaknesses in Tenable Exposure Management .....	817
Locate Connector Findings in Tenable Exposure Management .....	818
Data Mapping .....	820
Device Mapping .....	820
Finding Mapping .....	821
Finding Status Mapping .....	821
Finding Severity Mapping .....	822
Status Update Mechanisms .....	822
Uniqueness Criteria .....	823
API Endpoints in Use .....	823
Support and Expected Behavior .....	824
Data Validation .....	824
Asset Data Validation .....	824
Findings Data Validation .....	825





ServiceNow Connector .....	826
Connector Details .....	826
Prerequisites and User Permissions .....	827
Add a Connector .....	828
Configure the Connector .....	829
ServiceNow in Tenable Exposure Management .....	832
Locate Connector Assets in Tenable Exposure Management .....	832
Status Update Mechanisms .....	833
Uniqueness Criteria .....	834
API Endpoints in Use .....	834
Support Limitations and Expected Behavior .....	835
Data Validation .....	836
Asset Data Validation .....	836
Tanium Connector .....	841
Connector Details .....	842
Prerequisites and User Permissions .....	842
Add a Connector .....	843
Configure the Tanium Connector .....	844
Tanium in Tenable Exposure Management .....	846
Locate Connector Assets in Tenable Exposure Management .....	846
Locate Connector Weaknesses in Tenable Exposure Management .....	847
Locate Connector Findings in Tenable Exposure Management .....	848
Data Mapping .....	850
Device Mapping .....	850



Finding Mapping .....	851
Finding Status Mapping .....	851
Finding Severity Mapping .....	851
Status Update Mechanisms .....	852
Uniqueness Criteria .....	852
API Endpoints in Use .....	853
Support Limitations and Expected Behavior .....	853
Tenable On-Prem Connector .....	854
Prerequisites and User Permissions .....	854
Add a Connector .....	854
Configure the Connector .....	855
Veracode Connector .....	856
Connector Details .....	856
Prerequisites and User Permissions .....	857
Add a Connector .....	858
Configure the Connector .....	859
Veracode in Tenable Exposure Management .....	861
Locate Connector Assets in Tenable Exposure Management .....	861
Locate Connector Weaknesses in Tenable Exposure Management .....	862
Locate Connector Findings in Tenable Exposure Management .....	863
Data Mapping .....	865
Web Application Mapping .....	865
Finding Mapping .....	866
Finding Status Mapping .....	867



Finding Severity Mapping .....	867
Status Update Mechanisms .....	868
Uniqueness Criteria .....	868
Support and Expected Behavior .....	869
API Endpoints in Use .....	869
Data Validation .....	869
Asset Data Validation .....	869
Finding Data Validation .....	870
Wiz Vulnerabilities Connector .....	872
Connector Details .....	872
Prerequisites and User Permissions .....	873
Add a Connector .....	875
Configure the Connector .....	876
Wiz Vulnerabilities in Tenable Exposure Management .....	878
Locate Connector Assets in Tenable Exposure Management .....	878
Locate Connector Weaknesses in Tenable Exposure Management .....	879
Locate Connector Findings in Tenable Exposure Management .....	881
Data Mapping .....	882
Device Mapping .....	882
Device Finding Mapping .....	884
Container Mapping .....	885
Container Finding Mapping .....	887
Other Mapping .....	888
Other Finding Mapping .....	890



Finding Status Mapping .....	891
Finding Severity Mapping .....	891
Status Update Mechanisms .....	892
Uniqueness Criteria .....	892
API Endpoints in Use .....	893
Support Limitations and Expected Behavior .....	893
Data Validation .....	894
Asset Data Validation .....	894
Finding Data Validation .....	895
Wiz Cloud Configurations Connector .....	896
Connector Details .....	897
Prerequisites and User Permissions .....	897
Add a Connector .....	899
Configure the Connector .....	900
Wiz Vulnerabilities in Tenable Exposure Management .....	902
Locate Connector Assets in Tenable Exposure Management .....	902
Locate Connector Weaknesses in Tenable Exposure Management .....	903
Locate Connector Findings in Tenable Exposure Management .....	905
Data Mapping .....	906
Device Mapping .....	906
Device Finding Mapping .....	908
Container Mapping .....	909
Container Finding Mapping .....	911
Other Mapping .....	911



Other Finding Mapping .....	913
Finding Status Mapping .....	914
Finding Severity Mapping .....	914
Status Update Mechanisms .....	915
Uniqueness Criteria .....	915
API Endpoints in Use .....	916
Support Limitations and Expected Behavior .....	916
Data Validation .....	917
Asset Data Validation .....	917
Finding Data Validation .....	918
Wiz Issues Connector .....	919
Connector Details .....	919
Prerequisites and User Permissions .....	920
Add a Connector .....	922
Configure the Connector .....	923
Wiz Vulnerabilities in Tenable Exposure Management .....	925
Locate Connector Assets in Tenable Exposure Management .....	925
Locate Connector Weaknesses in Tenable Exposure Management .....	926
Locate Connector Findings in Tenable Exposure Management .....	928
Data Mapping .....	929
Device Mapping .....	929
Device Finding Mapping .....	931
Container Mapping .....	932
Container Finding Mapping .....	934



Other Mapping .....	935
Other Finding Mapping .....	936
Finding Status Mapping .....	937
Finding Severity Mapping .....	937
Status Update Mechanisms .....	938
Uniqueness Criteria .....	938
API Endpoints in Use .....	939
Support Limitations and Expected Behavior .....	939
Data Validation .....	940
Asset Data Validation .....	940
Finding Data Validation .....	941
Connector Scheduling .....	942
Configure Connector Scheduling .....	943
Expected Behaviour .....	943
Support and Limitations .....	944
Notes .....	944
Third-Party Data Deduplication in Tenable Exposure Management .....	944
Why Deduplication Matters .....	945
How it Works .....	945
Deduplication Criteria by Asset Class .....	945
Property Merge Order .....	946
Deduplication Limitations .....	948
Additional Resources .....	948
Asset Retention .....	948



Configuring Asset Retention .....	948
Tenable Exposure Management Cloud Sensors .....	949
Connectors FAQ .....	952
Integration and Support .....	953
Sync and Status .....	953
Deleted Connectors and Tags .....	954
Asset Deduplication FAQ .....	956
<b>Settings .....</b>	<b>959</b>
Exposure Management Settings .....	959



# Welcome to Tenable Exposure Management

Tenable Exposure Management helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to optimize business performance.

The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems, and builds on the speed and breadth of vulnerability coverage from Tenable Research and adds comprehensive analytics to prioritize actions and communicate cyber risk.

Tenable Exposure Management enables you to:

- Get comprehensive visibility of all assets and vulnerabilities, whether on-premises or in the cloud, and understand where they are exposed to risk.
- Anticipate threats and prioritize efforts to prevent attacks by using generative AI and the industry's largest dataset of vulnerability and exposure context.

**Note:** Generative AI is not supported in [Tenable FedRAMP Moderate](#) environments.

- Communicate exposure risk to business leaders and stakeholders with clear KPIs, benchmarks, and actionable insights.
- Leverage the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems.
- Integrate with third-party data sources and tools for enhanced exposure analysis and remediation.

**Tip:** For additional information on getting started with Tenable Exposure Management products, check out the [Tenable One Deployment Guide](#).

Tenable Exposure Management is an application that gathers data from the following Tenable products:

- [Tenable Vulnerability Management](#)
- [Tenable Security Center](#)





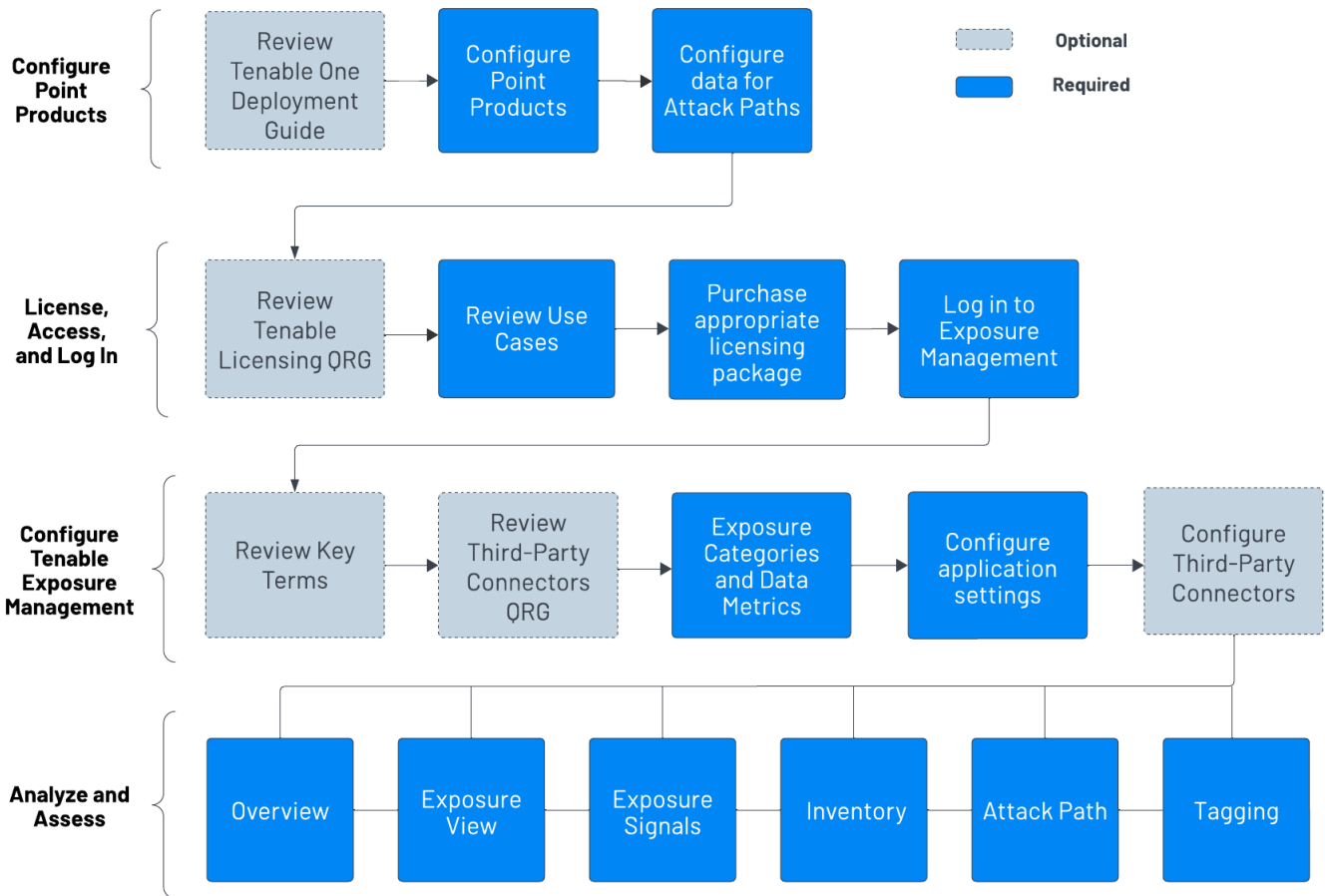
- [Tenable Web App Scanning](#)
- [Tenable Cloud Security](#)
- [Tenable Identity Exposure](#)
- [Tenable Attack Surface Management](#)
- [Tenable OT Security](#)

For more information, see [Get Started with Tenable Exposure Management](#).

## Get Started with Tenable Exposure Management

Tenable recommends following these steps to get started with Tenable Exposure Management data and functionality.

**Tip:** Click a box to view the relevant task.



## Configure your "Point Products" to get Data into Tenable Exposure Management

To get data into Tenable Exposure Management, you must first configure and deploy the Tenable Exposure Management "point products". Once these are configured, Tenable Exposure Management can then ingest the data and present it.

**Tip:** For additional information on getting started with Tenable Exposure Management products, check out the following resources:

- [Tenable One Deployment Guide](#)
- [Tenable One Introduction \(Tenable University\)](#)

For Attack Path data ingestion to function as expected, ensure you have the following:



- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
  - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** [scan template](#). This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

**Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

- [Tenable Identity Exposure](#) SaaS deployed.

**Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Tenable Exposure Management. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:
  - Have at least 40% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.
  - An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
  - When using Tenable Identity Exposure, enable [privileged analysis](#). This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
  - A scan frequency of at least once a week.
  - Configure Tenable OT Security.
  - Configure Tenable Attack Surface Management and [configure the application for use](#)



[with Tenable Vulnerability Management](#). This ensures that usable data gets pulled into Tenable Exposure Management.

## License, Access, and Log In

To use Tenable Exposure Management, you purchase licenses for assets: resources identified by – or managed in – your Tenable products. Each product has a different asset type. For more information, see the [Tenable One Licensing Quick-Reference Guide](#).

To acquire a license:

1. Determine the interface that best suits your business objectives. For more information, see [Tenable Exposure Management Use Cases](#).
2. Contact your Tenable representative to purchase the appropriate package.

To access and log in to Tenable Exposure Management:

- Review the [Tenable Exposure Management System Requirements](#).
- Follow the steps to [Log in to Tenable Exposure Management](#).

## Configure Tenable Exposure Management for Use

- Familiarize yourself with the Tenable Exposure Management [key terms](#).
- Familiarize yourself with the [categories and data metrics](#) within Tenable Exposure Management.

## Analyze and Assess

Perform analysis on your data within Tenable Exposure Management:

- Access the [Exposure View](#) page, where you can gain critical business context by getting business-aligned cyber exposure score for critical business services, processes and functions, and track delivery against SLAs. Track overall VM risk to understand the risk contribution of assets to your overall Cyber Exposure Score, including by asset class, vendor, or by tags.



- [View](#) and [manage](#) cyber exposure cards.
- View [CES](#) and [CES trend](#) data for any exposure card.
- View [Remediation Service Level Agreement](#) (SLA) data.
- View [Tag Performance](#) data.
- Access the [Exposure Signals](#) page, where you can generate exposure signals that use queries to search for asset *violations*. Simply put, if an asset is impacted by a weakness related to the query, then the asset is considered a *violation*. Using this, you can gain visibility into your most critical risk scenarios.
  - Find top active threats in your environment with up-to-date feeds from Tenable Research.
  - View, generate, and interact with the data from queries and their impacted asset violations.
  - Create custom exposure signals to view business-specific risks and weaknesses
- Access the [Inventory](#) page, where you can enhance asset intelligence by accessing deeper asset insights, including related attack paths, tags, exposure cards, users, relationships, and more. Improve risk scoring by gaining a more complete view of asset exposure, with an asset exposure score that assesses total asset risk and asset criticality.
  - View and interact with the data on the [Assets](#) tab:
    - Unify all assets in a single view to simplify analysis, understand relationships, and discover exposures across the attack surface.
    - Familiarize yourself with the [Global Asset Search](#) and its objects and properties. Bookmark custom queries for later use.
    - Find devices, user accounts, software, cloud assets, SaaS applications, networks, and their weaknesses.
    - Drill down into the [Asset Details](#) page to view asset properties and all associated context views.
  - View and interact with the data on the [Weaknesses](#) tab:



- View key context on vulnerability and misconfiguration weaknesses to make the most impactful remediation decisions.
- View and interact with the data on the [Software](#) tab:
  - Gain full visibility of the software deployed across your business and better understand the associated risks.
  - Identify what software may be out of date, and which pieces of software may soon be End of Life (EoL).
- View and interact with the data on the [Findings](#) tab:
  - View instances of weaknesses (vulnerabilities or misconfigurations) appearing on an asset, identified uniquely by plugin ID, port, and protocol.
  - Review insights into those findings, including descriptions, assets affected, criticality, and more to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.
- Access the [Attack Path](#) page, where you can optimize risk prioritization by exposing risky attack paths that traverse the attack surface, including web apps, IT, OT, IoT, identities, ASM, and prevent material impact. Streamline mitigation by identifying choke points to disrupt attack paths with mitigation guidance, and gain deep expertise with AI insights (**Not supported in [FedRAMP](#) environments**).
- View the [Dashboard](#) tab for a high-level view of your vulnerable assets such as the number of attack paths leading to these critical assets, the number of open attack techniques and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.
  - Review the **Top Attack Path Matrix** and click the **Top Attack Paths** tile to view more information about paths leading to your “Crown Jewels”, or assets with an ACR of 7 or above.

You can adjust these if needed to ensure you’re viewing the most critical attack path data.



- On the [Top Attack Techniques](#) tab, view all attack techniques that exist in one or more attack paths that lead to one or more critical assets by pairing your data with advanced graph analytics and the MITRE ATT&CK® Framework to create attack techniques, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.
- On the [Top Attack Paths](#) tab, generate attack path queries to view your assets as part of potential attack paths:
  - [Generate an Attack Path with a Built-in Query](#)
  - [Generate an Attack Path Query with the Attack Path Query Builder](#)
  - [Generate an Asset Query with the Asset Query Builder](#)

Then, you can view and interact with the [Attack Path Query](#) and [Asset Query](#) data via the query result list and the [interactive graph](#).

- Interact with the [MITRE ATT&CK Heatmap](#) tab.
- View and interact with the data in the [Tags](#) page:
  - [Create and manage tags](#) to highlight or combine different asset classes.
  - View the [Tag Details](#) page to gain further insight into the tags associated with your assets.
- Access the [Connectors](#) page, where you can view, manage, and add third-party connector integrations to Tenable Exposure Management. Tenable Exposure Management integrates with the vendor tool to pull asset and vulnerability data into the application and display it seamlessly alongside your Tenable application data. Once the integration is complete, the platform analyzes the data to correlate, consolidate, and contextualize the ingested data to impact risk and remediation priority.
  - [Create and manage connectors](#) to ingest your third-party application directly into Tenable Exposure Management.
  - View those connector [assets](#), [weaknesses](#), and [findings](#) on the **Inventory** page.

## Tenable Exposure Management Use Cases



The Tenable Exposure Management interface can be used in the following ways to support these common use cases:

User Type	Use Case
CISO/Executives	<p>Utilize the <a href="#">Exposure View</a> page to:</p> <ul style="list-style-type: none"><li>• Quickly quantify your overall enterprise risk exposure and identify which areas need further investigation.</li><li>• Create custom exposure cards to view data based on specific business contexts.</li><li>• Measure and prioritize risk exposure progress or regression.</li><li>• Easily communicate important risk information to teams and include in presentations.</li><li>• Understand how effective your program is via the <b>Remediation Maturity</b> metric.</li></ul>
Security Practitioner	<p>Utilize the <a href="#">Attack Path</a> page to:</p> <ul style="list-style-type: none"><li>• Evaluate the impact of insecure assets and communicate these insecurities to appropriate parties.</li><li>• Proactively identify hidden security issues within my assets and their relationships.</li></ul>
Both CISO/Executives and Security Practitioners	<p>Utilize the <a href="#">Exposure Signals</a> page to:</p> <ul style="list-style-type: none"><li>• Gain visibility into your most critical risk scenarios by viewing risk combinations of that could make any weakness potentially dangerous to your business</li><li>• Generate exposure signals that use queries to search for asset violations and view business-specific risks and weaknesses.</li></ul> <p>Utilize the <a href="#">Inventory</a> page to:</p> <ul style="list-style-type: none"><li>• View and manage all assets, regardless of their source.</li><li>• View and manage weaknesses across all of your vulnerability</li></ul>





findings.

- Consolidate data in one location, reducing license and maintenance costs

Utilize the [Tags](#) page to:

- Utilize existing tags or create new tags that can be used to create custom exposure cards.

## Licensing

This topic breaks down the Tenable One licensing process and lists the versions and components you can purchase. It also holds a [license calculator](#) with which you can estimate your license needs.


To learn how to use Tenable One, see [Tenable One Platform](#).

### Licensing Tenable One

To use Tenable One, you purchase licenses for *assets*: resources identified by—or managed in—your Tenable products. Some Tenable One products use different asset types. For example, in Tenable Web App Scanning, assets are unique fully qualified domain names (FQDNs), while in Tenable Identity Exposure, they are enabled users in your directory service. Once you have purchased licenses, your Tenable representative assigns them to your products based on the asset types you want to scan or manage.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

You can *reallocate* your licenses once per 90 days. For example, if you purchase 1,000 licenses and assign 500 each to Tenable Vulnerability Management and Tenable Security Center, you can switch 100 licenses to Tenable Vulnerability Management if your scan profile requires it. To reallocate licenses, contact your Tenable representative.

**Tip:** To view your current license count and available assets, in the Tenable top navigation bar, click  and then click **License Information**. To learn more, see [License Information Page](#).



**Note:** Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

## Tenable One Components

You can customize Tenable One for your use case by adding components. Some components are add-ons that you purchase.

**Tip:** The latest version of the platform is called **Tenable One**, but there were previously two versions: *Enterprise* and *Standard*. The following table lists all versions, but if you are a new customer, you will purchase **Tenable One**. If you have a Tenable One Standard or Enterprise quote, Tenable will honor it through the end of 2024. If you are a current customer, you can upgrade, downgrade, or renew as follows:

- **Current Tenable One Standard customers** – You can upgrade, downgrade, or renew the same version through the end of 2025.
- **Current Tenable One Enterprise customers** – You can upgrade, downgrade or renew the same version for the foreseeable future.

Version	Version Type	Included with Purchase	Add-on Component
<b>Tenable One</b>	Current version	<ul style="list-style-type: none"><li>• Tenable Security Center+ companion license.</li><li>• OT Security companion license.</li><li>• Tenable Web App Scanning on-premises companion license.</li></ul>	<ul style="list-style-type: none"><li>• If using Tenable Security Center, purchase additional consoles when you need more than three.</li><li>• Tenable Web App Scanning additional concurrency with Tenable cloud scanners.</li><li>• Tenable One Identity Exposure On-Premises.</li></ul>
<b>Tenable One</b>	Legacy	<ul style="list-style-type: none"><li>• Tenable Security</li></ul>	Tenable Web App Scanning



<b>Standard</b>	version	Center+ companion license. <ul style="list-style-type: none"><li>• OT Security companion license.</li><li>• Tenable Web App Scanning on-premises companion license.</li></ul>	additional concurrency with Tenable cloud scanners.
<b>Tenable One Enterprise</b>	Legacy version	<ul style="list-style-type: none"><li>• Tenable Security Center+ companion license.</li><li>• OT Security companion license.</li><li>• Tenable Web App Scanning on-premises companion license.</li></ul>	<ul style="list-style-type: none"><li>• If using Tenable Security Center, purchase additional consoles when you need more than three.</li><li>• Tenable Web App Scanning additional concurrency with Tenable cloud scanners.</li><li>• Tenable Attack Surface Management Daily Frequency.</li></ul>

## Tenable One Asset Values

Tenable One has a centralized platform approach, collecting data from many asset types and providing domain-specific security teams (for example, Tenable Vulnerability Management, Tenable Cloud Security) with specialized domain-specific applications. These applications are similar to point products for managing cloud, web applications, OT assets, and so on, enhanced with context from the Tenable One platform.



The value customers derive from Tenable One varies by the type of resource being managed, as does the cost incurred by Tenable. To align Tenable One pricing to value, Tenable converts the number of different resource types (for example, web servers, cloud resources, OT devices) to a number of Tenable One assets based on ratios defined in the following table. In this way we maintain a single price per Tenable One asset no matter the variety of resources being managed.

## Reclaiming Licenses

When you purchase Tenable licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable One products reclaim licenses under some conditions—and then reassign them to new assets in the same product so that you do not run out of licenses.

## Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable One licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Exposure Management.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Exposure Management.
You scan more assets than are licensed for 30+ days.	A message appears in Tenable Exposure Management; scan and export features are disabled.

**Tip:** Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see [Scan Best Practices](#).

## Expired Licenses

The Tenable One licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.



After your license expires, you can no longer sign in to the Tenable platform.

## Tenable Exposure Management System Requirements

### Display Settings

Minimum screen resolution: 1440 x 1024

### Supported Browsers

Tenable Exposure Management supports the latest versions of the following browsers.

**Note:** Before reporting issues with Tenable Exposure Management, ensure your browser is up to date.

- Google Chrome
- Apple Safari
- Mozilla Firefox
- Microsoft Edge

**Note:** Tenable Exposure Management is not supported on mobile browsers.

### Key Terms

The following key terms apply to the Tenable Exposure Management user interface.

Term	Definition
Active Directory (AD)	Tenable Exposure Management integrates AD data from Tenable Identity Exposure.
Asset	Any IT or security element in your organization such as user accounts, computers, and software. The <b>Discover</b> section represents an asset as a node in the graph.
Asset Exposure Graph	A visualization of an attack path from multiple assets down to one asset.



Asset Exposure Score (AES)	Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure
Asset Vulnerability Rating (AVR)	An aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on an asset.
Benchmark	A group of scores to which you can compare your scores and assess your performance.
Blast Radius	A visualization of one or more attack paths from one asset to multiple other assets.
CES Trend	A measurement that defines how your CES improves or regresses over time.
Chief Information Security Officer (CISO)	The head of cybersecurity for a company. A CISO can use the Exposure View to quickly quantify the overall enterprise risk exposure, measure its progress or regression over time and easily communicate impact and ROI to key stakeholders.
Choke Point Priority	A choke point is a place where potential attack paths merge together before reaching a critical asset. Tenable Exposure Management uses Choke Point Priority as a prioritization metric for attack techniques based on the number of attack paths exploiting the attack, the number of critical assets it leads to, and complexity of the attack. Tenable Exposure Management categorizes priority levels as <b>Low</b> , <b>Medium</b> , <b>High</b> , and <b>Critical</b> . Tenable recommends focusing on areas with higher choke points first, as remediating those will negate the largest number of critical items within your organization.
Cyber Exposure Score (CES)	Your CES quantifies the relative risk of your organization based on the threat exposure and criticality of your licensed assets. CES values range from 0 - 1000, where higher values indicate higher exposure and higher risk.
Data Source	A product that feeds data into Tenable Exposure Management (for example,



	Tenable Vulnerability Management).
Evidence	The empirical data from different data sources confirming the feasibility of a <a href="#">Step</a> as part of an attack path.
Exposure Card	An Exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your Cyber Exposure Score (CES) and other metrics. Users can create custom cards, or use Tenable-provided cards to gain insight and guidance on what areas need their attention most.
Exposure Card View	The section of the Exposure View that includes data about the selected exposure card. This section includes CES, trend, Remediation SLA, and business context information.
Exposure View	A holistic and unified view combining internal and external data sources to provide a complete view of risk in a singular location.
Finding	A single instance of a vulnerability appearing on an asset, uniquely identified by plugin ID, port, and protocol.
Industry Benchmark	A benchmark based on members of your Tenable-assigned industry to which you can compare your scores and assess your performance.
MITRE ATT&CK®	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
Node Exposure Score (NES)	A metric produce by Tenable Exposure Management to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
Path Priority Rating	A prioritization metric for attack paths based on the exposure of the source, criticality of the target and the number of steps of the attack path.



Population Benchmark	A benchmark based on members of the entire population to which you can compare your scores and assess your performance.
Query Builder	A customizable visualization of one or more attack paths based on configurable source and target assets.
Query Library	Predefined queries that visualize scenarios of potential attack paths based on real-world attacks.
Operational Technology (OT)	Tenable Exposure Management integrates OT data from OT Security.
Security Practitioner	A Security Practitioner can use the Asset Inventory to evaluate the impact of unsecured assets, proactively identify hidden security issues in assets relationships, and quickly locate areas where a breach or risk is likely to happen.
Service Level Agreement (SLA)	A control by which you can identify whether assets comply with customer security requirements.
Step	A feasible implementation of a technique or sub-technique in an attack path that an adversary can leverage. The <a href="#">Top Attack Paths</a> view illustrates a step as a "bracket" between two or more assets.
Technique / Sub-Technique	Represents "how" an adversary achieves a tactical goal by performing an action. For example, an adversary can dump credentials to achieve credential access.
Tags	A way to group assets by business context. For example, you can group assets by product, permissions, business owner, etc.
Third Party Asset	A host, code project, image, website, or cloud resource ingested from a non-Tenable source.
Top Attack Path	An attack path that leads to one or more critical assets.
Vulnerability Management	Tenable Exposure Management integrates VM data from Tenable Vulnerability Management and Tenable Security Center.





(VM)	
Web Application Scanning (WAS)	Tenable Exposure Management integrates web app scanning data from Tenable Web App Scanning.

## Data Sources

A data source is any product that feeds data into the Tenable Exposure Management interface. Once you have configured a data source for use with Tenable Exposure Management, the application automatically ingests data from that Tenable Exposure Management product.

You can configure the following Tenable products as data sources:

- [Tenable Vulnerability Management](#)
- [Tenable Security Center](#)
- [Tenable Web App Scanning](#)
- [Tenable Cloud Security](#)
- [Tenable Identity Exposure](#)
- [Tenable Attack Surface Management](#)
- [Tenable OT Security](#)

To configure Tenable Vulnerability Management data sources:

1. Deploy Tenable Vulnerability Management according to the [steps](#) outlined in the *Tenable Vulnerability Management User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. [Configure Tenable Vulnerability Management](#) for use with Tenable Exposure Management by:
  - Creating and applying asset tags
  - Creating and launching scans to generate asset data

**Tip:** For more detailed information on configuring Tenable Vulnerability Management for use with Tenable Exposure Management, see the [Tenable Vulnerability Management](#) topic in the *Tenable Exposure Management Deployment Guide*.



## To configure Tenable Security Center data sources:

1. Deploy Tenable Security Center according to the [steps](#) outlined in the *Tenable Security Center User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. Once you have installed Tenable Security Center, follow the [Tenable Exposure Management Synchronization](#) steps outlined in the *Tenable Security Center User Guide*.

**Tip:** For more detailed information on configuring Tenable Security Center for use with Tenable Exposure Management, see the [Tenable Security Center](#) topic in the *Tenable Exposure Management Deployment Guide*.

## To configure Tenable Web App Scanning data sources:

1. Deploy Tenable Web App Scanning according to the [steps](#) outlined in the *Tenable Web App Scanning User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. [Create some quick scans](#) to provide a high-level assessment of the target to establish your baseline.

**Tip:** For more detailed information on configuring Tenable Web App Scanning for use with Tenable Exposure Management, see the [Tenable Web App Scanning](#) topic in the *Tenable Exposure Management Deployment Guide*.

## To configure Tenable Cloud Security data sources:

Deploy Tenable Cloud Security according to the [steps](#) outlined in the *Tenable Cloud Security User Guide*, or based on guidelines received directly from Tenable Professional Services.

**Tip:** For more detailed information on configuring Tenable Cloud Security for use with Tenable Exposure Management, see the [Tenable Cloud Security](#) topic in the *Tenable Exposure Management Deployment Guide*.

## To configure Tenable Identity Exposure data sources:

1. If necessary, [activate Tenable Identity Exposure](#) for use within your Tenable Exposure Management platform.
2. Deploy Tenable Identity Exposure according to the [steps](#) outlined in the *Tenable Identity Exposure User Guide*, or based on guidelines received directly from Tenable Professional Services.



3. [Configure Tenable Identity Exposure](#) for use with Tenable Exposure Management by:
  - Downloading and configuring the license file
  - Downloading and installing the Secure Relay
  - Configuring Forests

**Tip:** For more detailed information on configuring Tenable Identity Exposure for use with Tenable Exposure Management, see the [Tenable Identity Exposure](#) topic in the *Tenable Exposure Management Deployment Guide*.

## To configure Tenable Attack Surface Management data sources:

**Important:** Tenable Exposure Management only imports asset data from Tenable Attack Surface Management.

1. Deploy Tenable Attack Surface Management according to the [steps](#) outlined in the *Tenable Attack Surface Management User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. [Configure the application for use with Tenable Vulnerability Management](#). This ensures that usable data gets pulled into Tenable Exposure Management.
3. [Configure Tenable Attack Surface Management](#) for use with Tenable Exposure Management by:
  - Configuring domains within Tenable Attack Surface Management
  - Configuring data sets and confirming your entire attack surface is present

**Tip:** For more detailed information on configuring Tenable Attack Surface Management for use with Tenable Exposure Management, see the [Tenable Attack Surface Management](#) topic in the *Tenable Exposure Management Deployment Guide*.

## To configure Tenable OT Security data sources:

1. Install the Tenable OT Security appliance according to the [steps](#) outlined in the *Tenable OT Security User Guide*.
2. (Optional) If you want to pair your sensors with the Industrial Core Platform (ICP), install the OT Security Sensor according to the [steps](#) outlined in the *Tenable OT Security User Guide*.



3. Generate a Tenable OT Security **Linking Key** and determine your **Cloud Site** according to the [steps](#) outlined in the *Tenable Vulnerability Management User Guide*. Copy and save this information to link the connector to Tenable Exposure Management.
4. Integrate your Tenable OT Security appliance with Tenable Exposure Management according to the [steps](#) outlined in the *Tenable OT Security User Guide*.

**Tip:** For more detailed information on configuring Tenable OT Security for use with Tenable Exposure Management, see the [Tenable OT Security](#) topic in the *Tenable Exposure Management Deployment Guide*.

## Data Timing

Data within Tenable Exposure Management refreshes on the following cadence:

- Asset Data – Asset information is updated every time the asset is seen as part of a scan.
- Tag Application – When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of assets and the tag's rules.
- Tag Reevaluation – Every 12 hours, Tenable Exposure Management automatically reevaluates tags to ensure they apply to newly discovered assets, and are removed from any inactive assets.
- Tenable Cloud Security data – Tenable Exposure Management automatically refreshes Tenable Cloud Security data every 24 hours.

## Tenable Exposure Management Metrics

The following metrics are used to assess data within Tenable Exposure Management:

### Data Timing

Data within Tenable Exposure Management refreshes on the following cadence:

- Asset Data – Asset information is updated every time the asset is seen as part of a scan.
- Tag Application – When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of assets and the tag's rules.



- Tag Reevaluation – Every 12 hours, Tenable Exposure Management automatically reevaluates tags to ensure they apply to newly discovered assets, and are removed from any inactive assets.
- Tenable Cloud Security data – Tenable Exposure Management automatically refreshes Tenable Cloud Security data every 24 hours.

## Cyber Exposure Score (CES)

Tenable Exposure Management calculates a dynamic CES that represents exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for assets. Higher CES values indicate higher risk.

**Note:** Tenable Exposure Management does not include assets older than 90 days in your CES.

CES Category	CES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

## Asset Exposure Score (AES)

Tenable Exposure Management calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

**Note:** Tenable Exposure Management does not calculate an AES for unlicensed assets.

AES Category	AES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

## Asset Criticality Rating (ACR)



Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.

ACR Category	ACR Range
Critical	9 to 10
High	7 to 8
Medium	4 to 6
Low	1 to 3

## Vulnerability Priority Rating (VPR)

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

**Note:** Vulnerabilities without CVEs (for example, many vulnerabilities with the **Info** severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

## Exposure Categories

Tenable Exposure Management products refer to data sources as *Exposure Categories*. Tenable Exposure Management uses specific icons to represent these within the user interface.

**Tip:** For more information about the data sources related to these categories, see [Data Sources](#).



Exposure Category	Icon
Vulnerability Management	
Web Applications	
Identity Exposure	
Operational Technologies	
Cloud Security	

## Scoring Caveats within Tenable Exposure Management

The weakness counts and severities within the [Asset Details](#) tab and other areas within the Tenable Exposure Management user interface may not match because each segment counts instances differently:

For Tenable Vulnerability Management assets:

- Weakness counts: Are distinct CVE counts
- Exposure score counts: Distinct (plugin ID, CVE ID) counts to allow for recasted plugins to affect exposure scores

For Tenable Web App Scanning assets:

- Weakness counts: Number of distinct CVEs + distinct plugins where the plugin has no CVEs but has a VPR
- Exposure score counts: Distinct plugin ID counts with VPR > 0. This is to account for plugin ID vulnerabilities with no CVE and to allow for recasted plugins to affect exposure scores

For Tenable Identity Exposure assets:

- Weakness counts: Distinct IoEs observed directly on the asset
- Exposure score counts: Includes IoEs observed directly on the asset plus those inherited from related assets to account for inherited IoEs in exposure scores

For Tenable Cloud Security assets:



- Weakness counts: Cloud Security misconfigurations plus any CVEs found on the asset
- Exposure score counts: Only Cloud Security misconfigurations are counted for exposure scores.

## Log in to Tenable Exposure Management

To log in to Tenable Exposure Management:

1. In a supported browser, navigate to <https://cloud.tenable.com/>. The login page appears.
2. Type your **Username** and **Password** credentials.
3. Click **Login**.

The **Workspace** page appears.

4. Click the Tenable Exposure Management tile.

The Tenable Exposure Management interface appears. By default, you navigate directly to the [Home](#) page.

**Tip:** Don't see the tile you're looking for? You may need a license for that application. See the [Tenable Licensing Guide](#) or contact your Tenable representative for more information.

## Navigate Tenable Exposure Management

Tenable Exposure Management includes several helpful shortcuts and tools that highlight important information and help you to navigate the user interface more efficiently:

### Resource Center

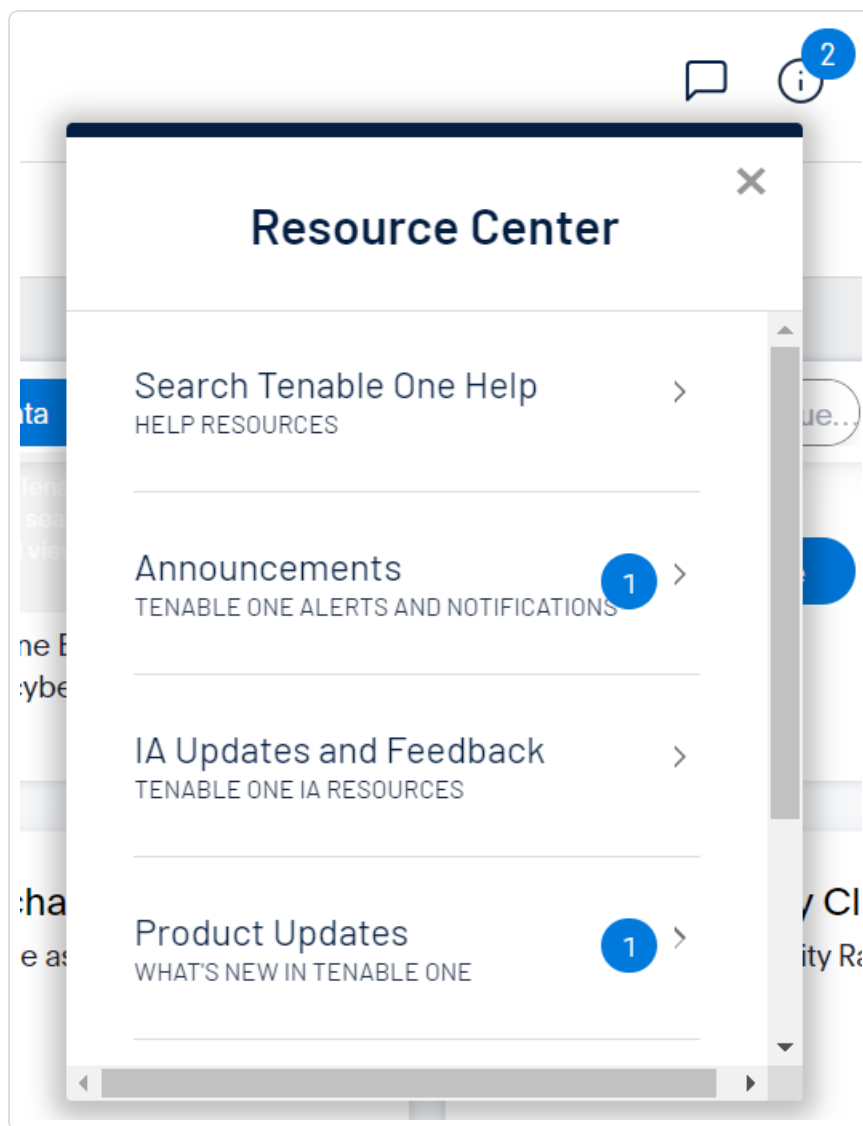
The **Resource Center** displays a list of informational resources including product announcements, Tenable blog posts, and user guide documentation.

To access the Resource Center:

1. In the upper-right corner, click the ⓘ button.


The **Resource Center** menu appears.





2. Click a resource link to navigate to that resource.

## Notifications

In Tenable Exposure Management, the **Notifications** panel displays a list of system notifications. The  button shows the current number of unseen notifications. When you open the **Notifications** panel, Tenable Exposure Management marks those notifications as seen. Once you have seen a notification, you can clear it to remove it from the **Notifications** panel.

**Note:** Tenable Exposure Management groups similar notifications together.


To view notifications:



- In the upper-right corner, click the  button.

The **Notifications** panel appears and displays a list of system notifications.

In the **Notifications** panel, you can do the following:

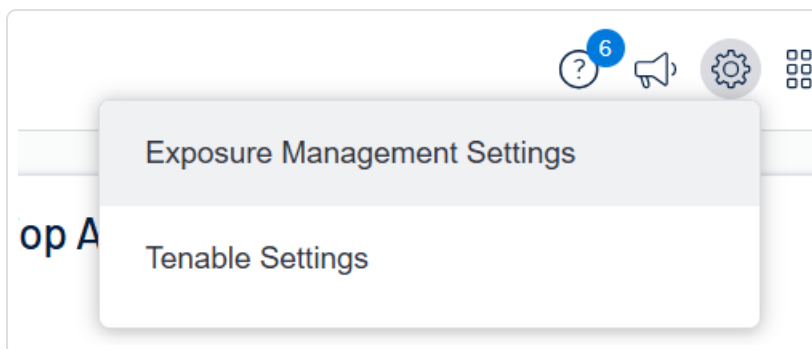
- To clear one notification, next to the notification, click the  button.
- To expand a group of notifications, at the bottom of the grouped notification, click **More Notifications**.
- To collapse an expanded group of notifications, at the top of the expanded notifications, click **Show Less**.
- To clear an expanded group of notifications, at the top of the expanded notifications, click **Clear Group**.
- To clear all notifications, at the bottom of the panel, click **Clear All**.

## Settings

To manage your settings:

1. In the upper-right corner, click the  button.

A menu appears.



2. Do one of the following:

- To manage your Tenable Exposure Management settings, click **Exposure Management Settings**.

The **Exposure Management Settings** page appears. For more information, see [Exposure Management Settings](#).



- To manage your Tenable One platform settings, click **Tenable Settings**.

You navigate directly to the **Settings** page within Tenable Vulnerability Management. For more information, see [Settings](#) in the *Tenable Vulnerability Management User Guide*.

## Workspace

When you log in to Tenable, the **Workspace** page appears by default. On the **Workspace** page, you can switch between your Tenable applications or set a default application to skip the **Workspace** page in the future. You can also switch between your applications from the **Workspace** menu, which appears in the top navigation bar.

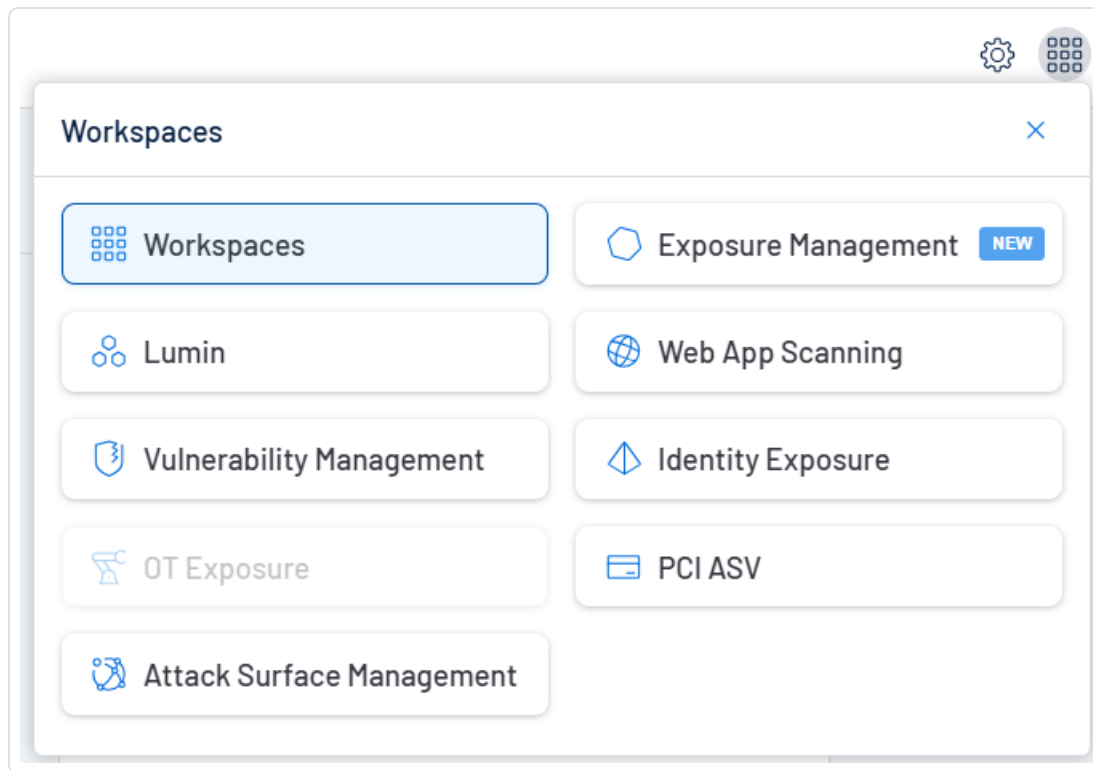
**Important:** Tenable disables application tiles for expired applications. Tenable removes expired application tiles from the **Workspace** page and menu 30 days after expiration.

## Open the Workspace Menu

To open the **Workspace** menu:

1. From any Tenable application, in the upper-right corner, click the  button.


The **Workspace** menu appears.



2. Click an application tile to open it.

## View the Workspace Page

To view the Workspace page:

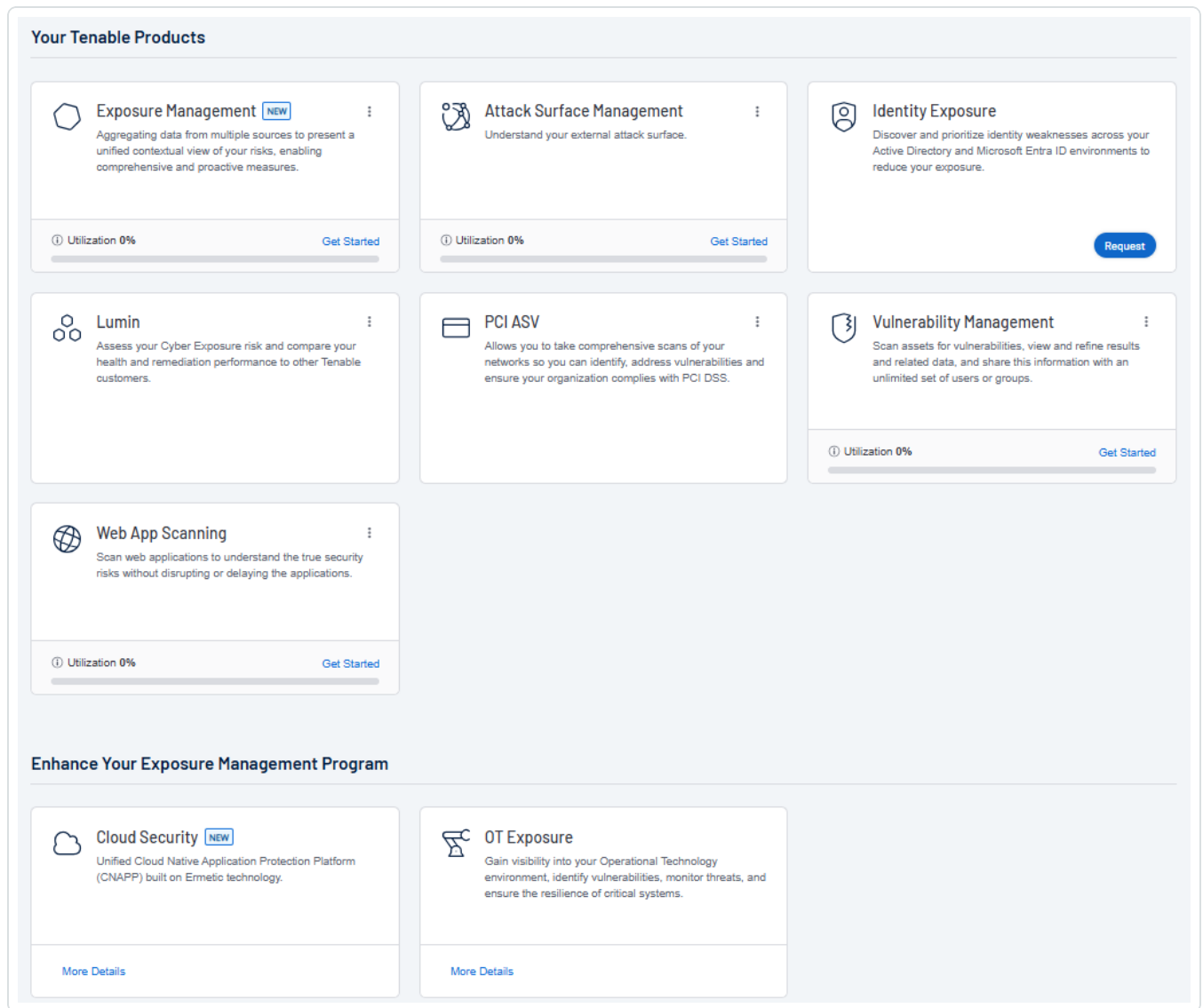
1. From any Tenable application, in the upper-right corner, click the  button.

The **Workspace** menu appears.

2. In the **Workspace** menu, click **Workspaces**.



The **Workspace** page appears.



On the **Workspace** page, you can do the following:

- Where applicable, at the bottom of a tile, view the percentage of your license utilization for the application. Click **See More** to navigate directly to the **License Information** page for the selected application.

**Tip:** For more information on how Tenable licenses work and how assets or resources are licensed in each product, see [Licensing Tenable Products](#).

- Set a default application:



When you log in to Tenable, the **Workspace** page appears by default. However, you can set a default application to skip the **Workspace** page in the future.

By default, users with the **Administrator**, **Scan Manager**, **Scan Operator**, **Standard**, and **Basic** roles can set a default application. If you have another role, contact your administrator and request the **Manage** permission under **My Account**. For more information, see [Custom Roles](#).

To set a default login application:

1. In the top-right corner of the application to choose, click the **:** button.

A menu appears.

2. In the menu, click **Make Default Login Page**.

This application now appears when you log in.

- **Remove a Default Application:**

To remove a default login application:

1. In the top-right corner of the application to remove, click the **:** button.

A menu appears.

2. Click **Remove Default Login Page**.

The **Workspace** page now appears when you log in.

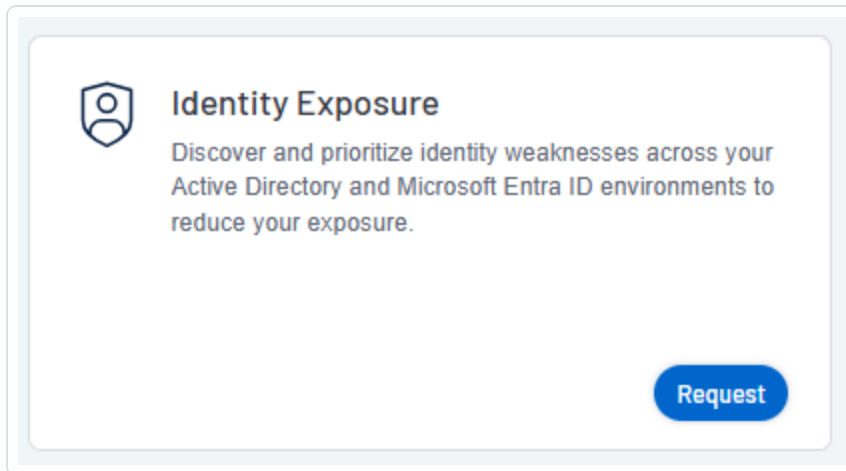
- **Request Access to a Tenable application:**

Some applications, like Tenable Identity Exposure, require you to request access to the application. You can do this directly via the **Workspace** page.

To request access to a Tenable application:



1. In the lower-right corner of the tile, click **Request**.



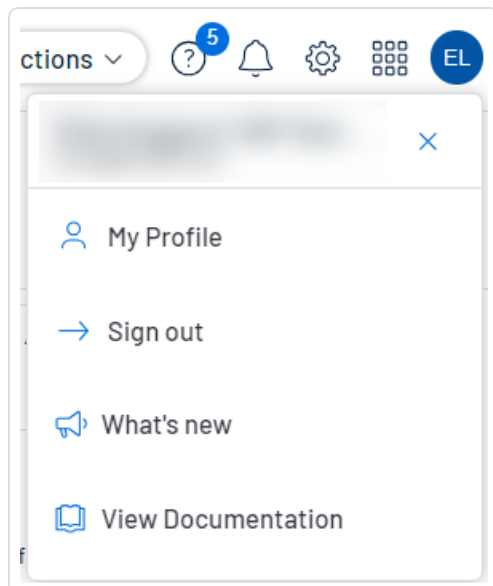
You navigate directly to the request page for the selected application.

## User Account Menu

The user account menu provides several quick actions for your user account.

1. In the upper-right corner, click the blue user circle.

The user account menu appears.





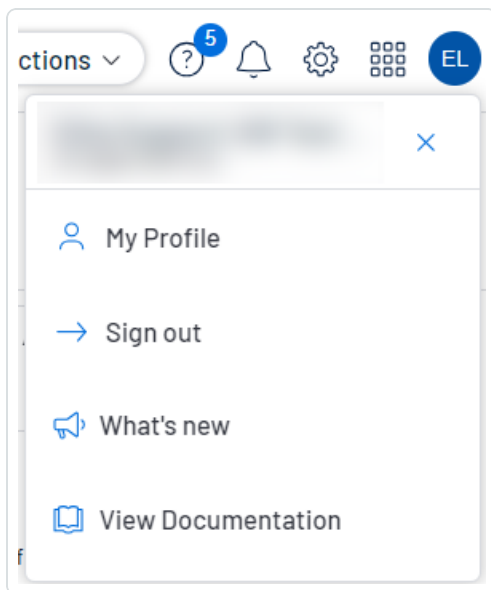
2. Do one of the following:

- Click **My Profile** to configure your own user account. You navigate directly to the **My Account** settings page.
- Click **Sign out** to sign out of Tenable Exposure Management.
- Click **What's new** to navigate directly to the Tenable Exposure Management Release Notes.
- Click **View Documentation** to navigate directly to the Tenable Exposure Management User Guide documentation.

## Log out of Tenable Exposure Management

To log out of Tenable Exposure Management:

1. In the upper right corner of any page, access the user account menu.



2. Click **Sign Out**.





# Home

---

The **Home** page within Tenable Exposure Management allows you to gain a comprehensive understanding of your data. The goal is to position you to take proactive measures by surfacing the most relevant Key Performance Indicators (KPIs) in a unified, holistic view.

On the **Home** page, you can get an at-a-glance idea of:

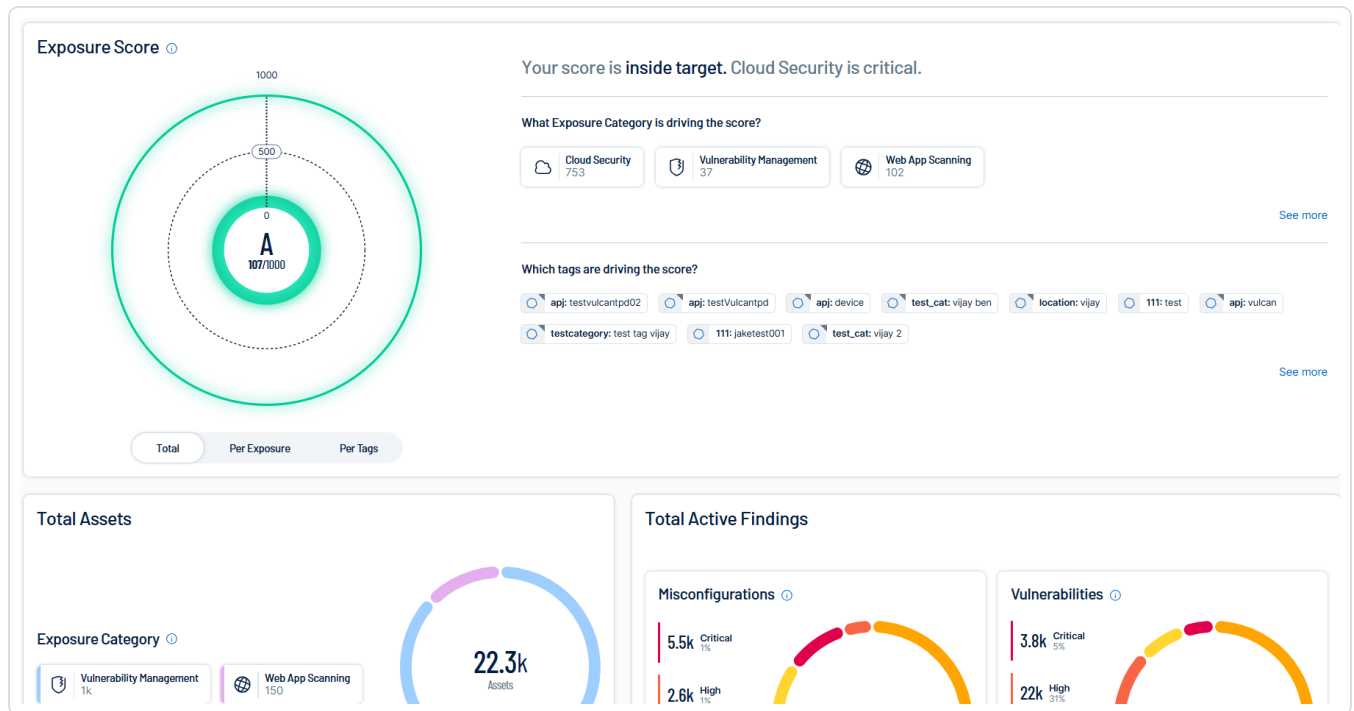
- Your key drivers:
  - What [exposure categories](#) are driving your score, and by how much?
  - Which tag(s) are driving your score, and by how much?
- Your assets:
  - What sources are your assets coming from?
  - Navigate directly to the [Assets](#) page for a deeper dive into asset data.
- Your findings:
  - What sources are your findings coming from?
  - Navigate directly to the [Findings](#) page for a deeper dive into finding data.

To access the Home page:



1. Log in to Tenable Exposure Management.

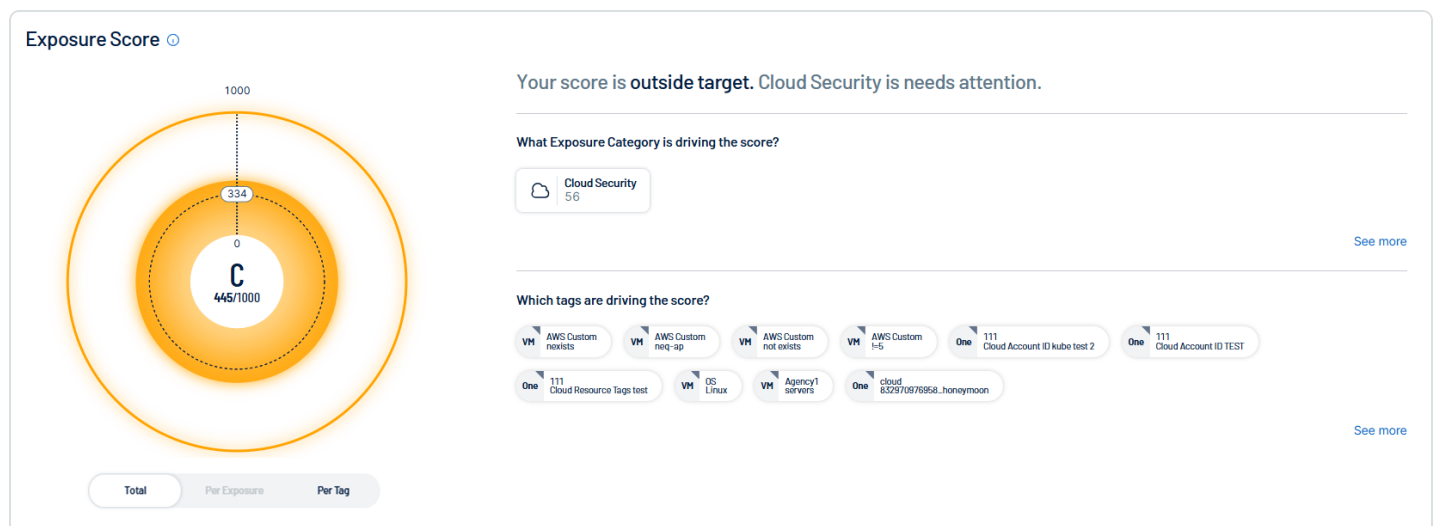
By default, the **Home** page appears.



The **Home** page includes the following sections:

## Exposure Score

The **Exposure Score** section displays your **Global** Cyber Exposure Score.

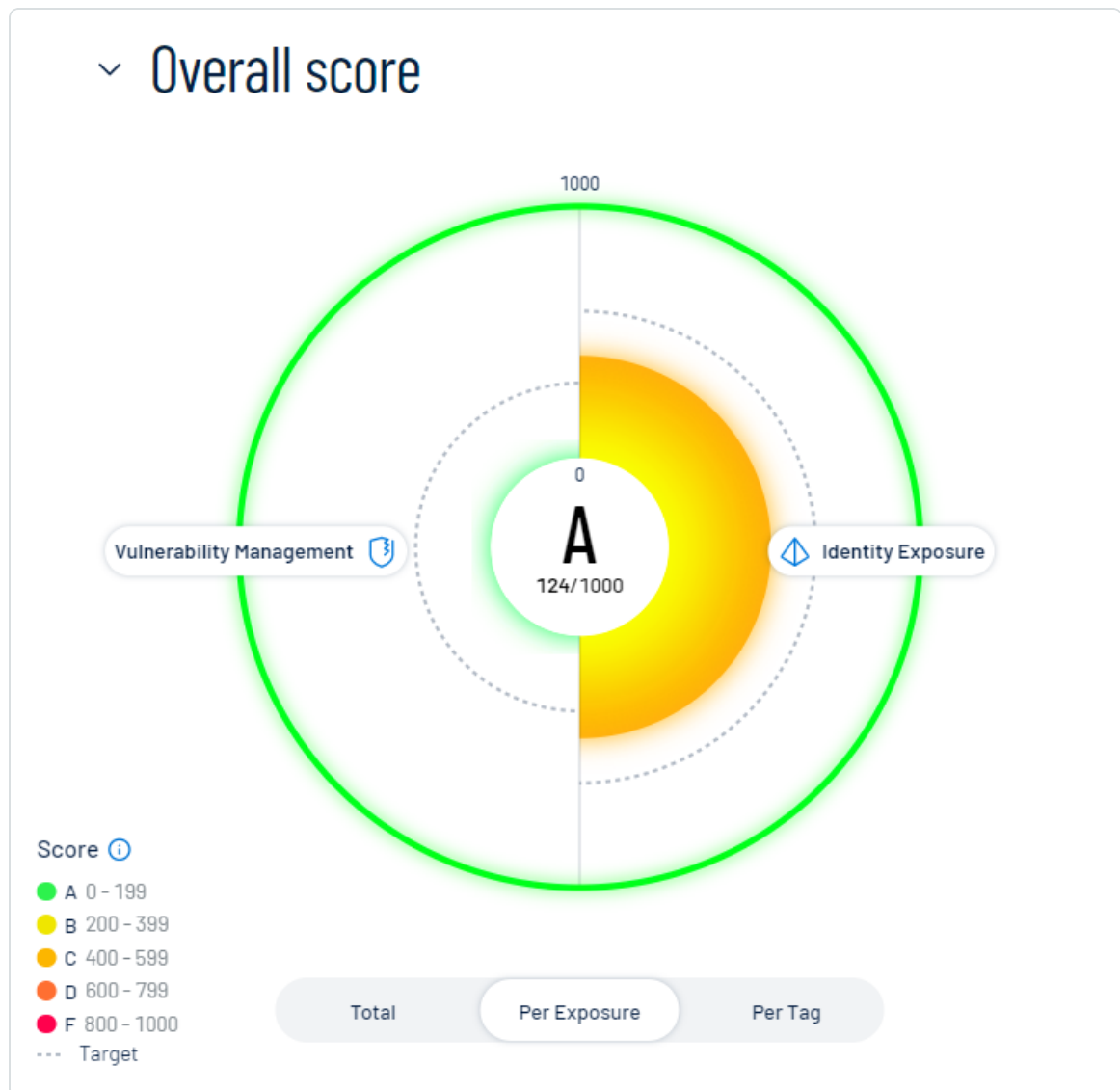


Here, you can:

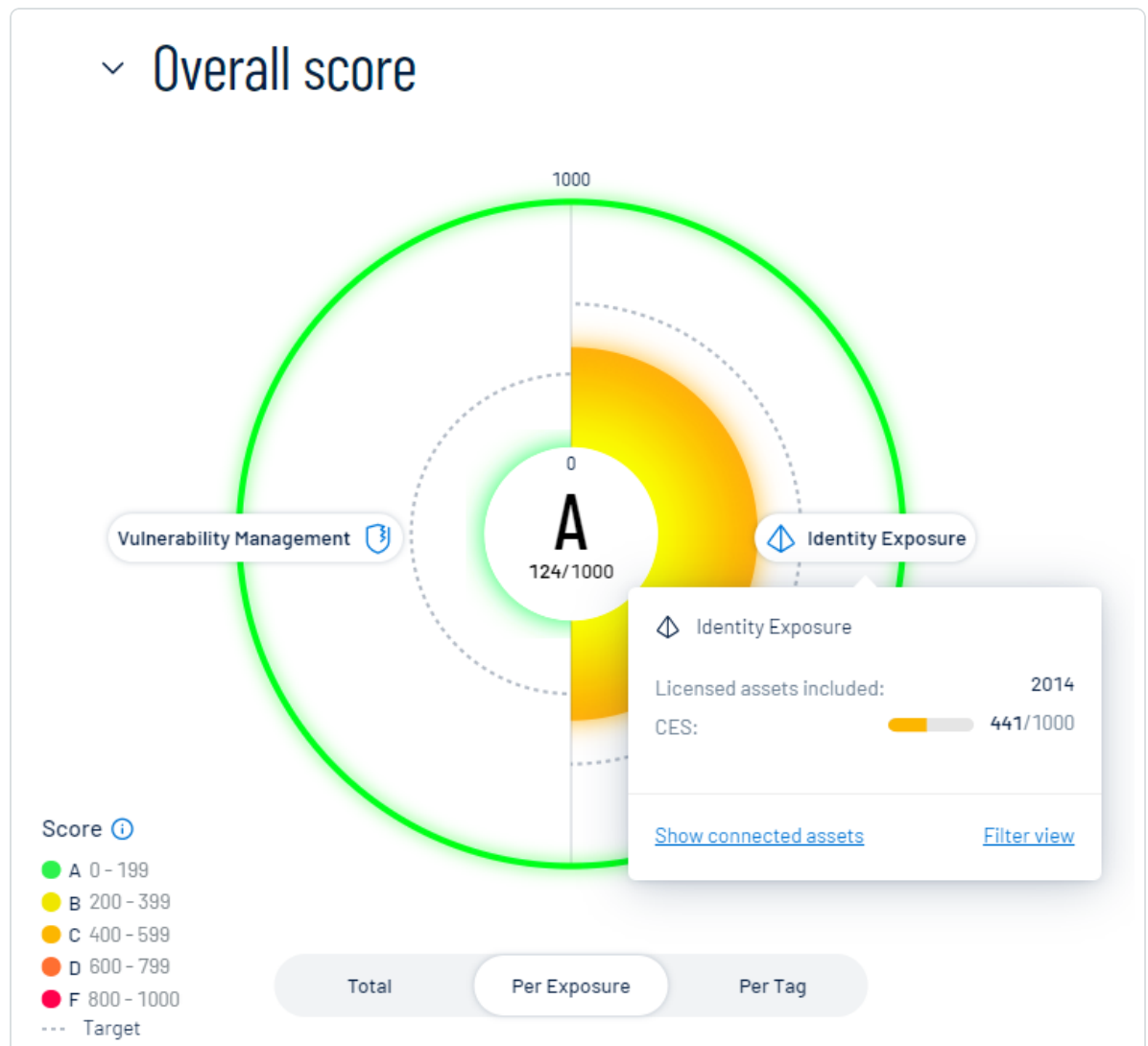


- View a graphical representation of your CES grade as it compares to your industry and the total population:
  - To view your total CES regardless of the data source, below the circle graph, click **Total**.
  - To view your CES separated based on the source of the exposure, below the circle graph, click **Per Exposure**.

The CES graph splits into sections that represent each exposure source, for example, **Identity Exposure**. For more information, see [Tenable Exposure Management Metrics](#).



- Within the CES graph, click an individual category name to view additional category information, [connected assets](#), and to filter the page by the selected category.



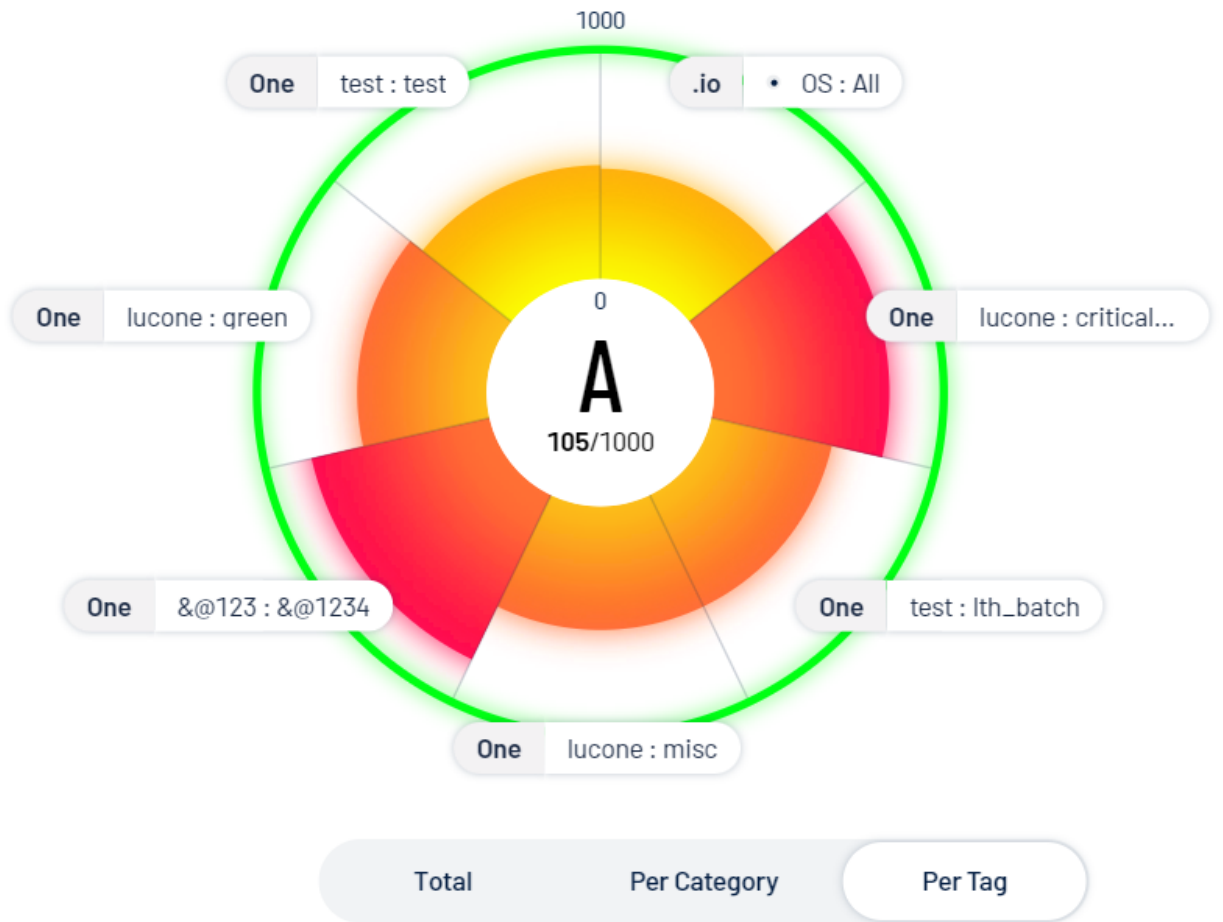
- To view the top tags driving your score, below the circle graph, click **Per Tag**.

**Note:** Tenable Exposure Management displays up to 10 tags within the graph.

The CES graph splits into sections that represent each tag. For more information on tags, see [Tags](#).

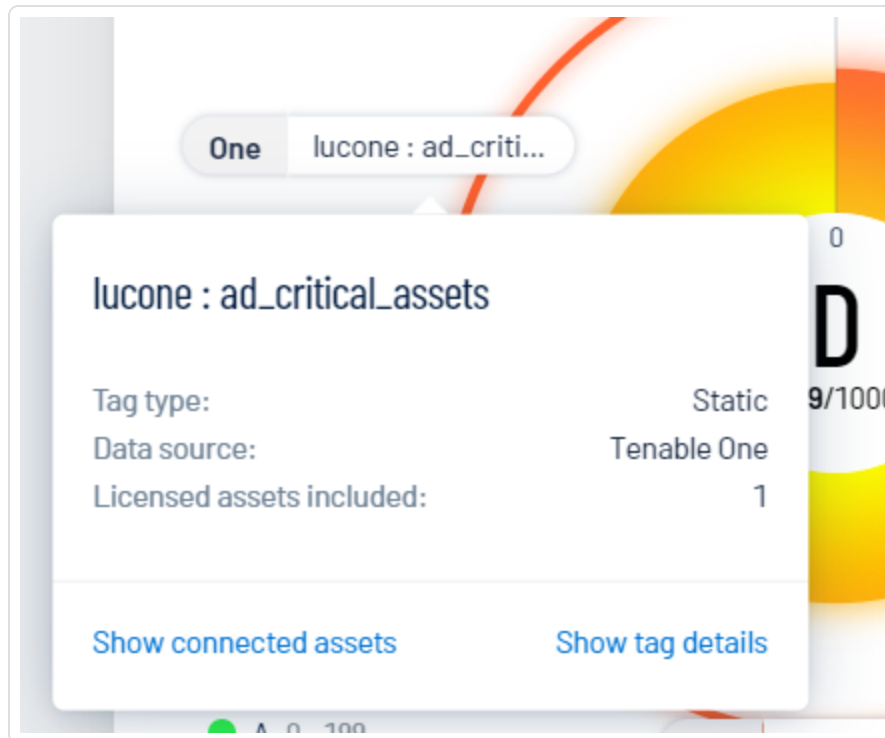


## Overall score





- Within the CES graph, click an individual tag name to view additional tag information, [connected assets](#), and [tag details](#).



- To the right of the CES graph, you can view the following information:
    - How your score compares to the baseline target.
    - The performance of your categories. For example, this blurb may explain that you have two critical categories.
    - Which [exposure management classes](#) are driving your score, for example, **Cloud Security**.
      - For more information, click **See More**.
- Tenable Exposure Management navigates you directly to the [Exposure View](#) page, where you can view additional information about your CES and its changes and trends over time.
- A list of which [tags](#) are driving your score.



- For more information, click **See More**.

Tenable Exposure Management navigates you directly to the [Tags](#) page, where you can view and manage all of your Tenable Exposure Management tags and the assets to which they are applied.

### Top Attack Path Matrix

The **Top Attack Path Matrix** section of the **Home** page includes a matrix that shows the number of attack paths corresponding to target Asset Criticality Rating (ACR) and Source Node Exposure Score values. This matrix includes only assets with an ACR of 7 or higher to ensure you can prioritize your most critical assets first.

**Tip:** At the top of the matrix, click on a **Data Source** to filter the matrix by attack paths from the selected source. If there is no data available for a data source type, the button for that source is disabled.



## Top Attack Path Matrix ⓘ

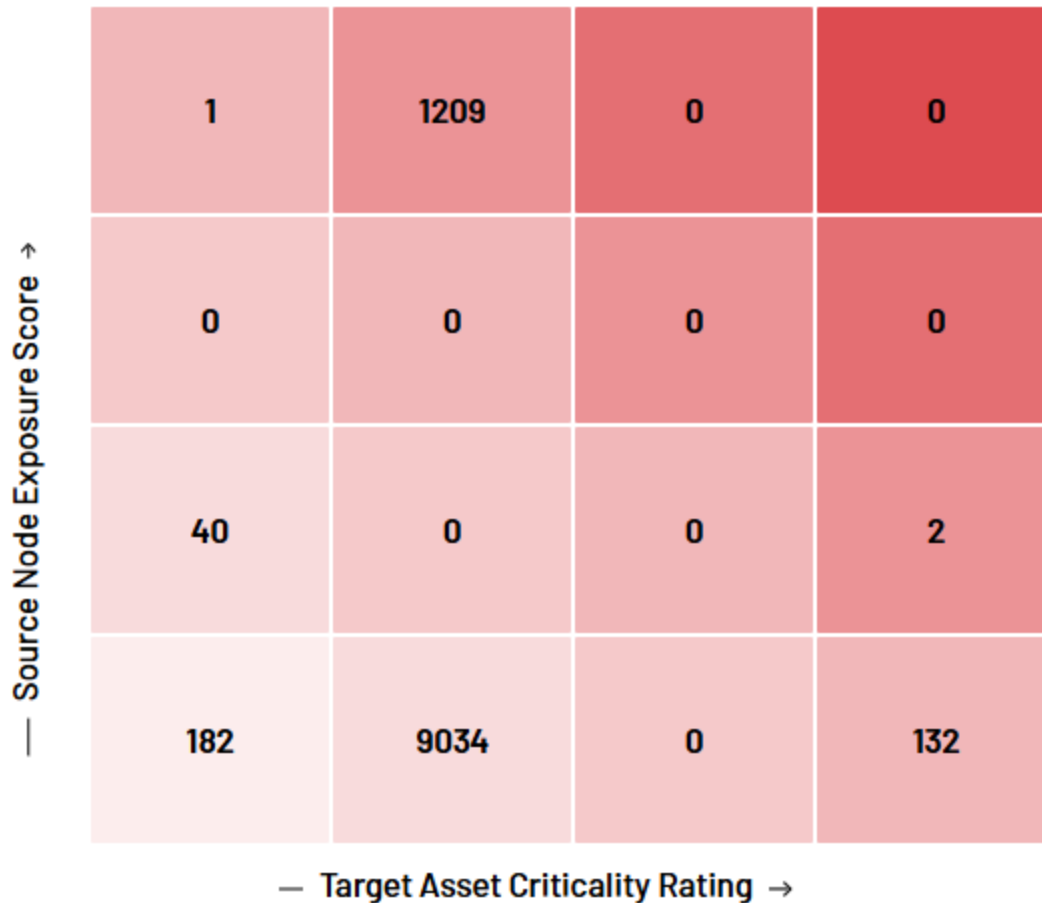
Data Source:

Global

VM

IE

...



Source NES Range: Low: 0 to <4 Medium: 4 to <7 High: 7 to <9 Critical: 9 to 10

Target ACR Range: Low to High: 0 to <8 High: 8 to <9 Critical: 9 to <10 Critical: 10

Here, you can:

- Quickly view the attack paths that lead to the highest ACR targets and whose source nodes have the highest exposure score source by checking the value in the square in the upper right corner of the matrix.
- Click any square to navigate to the [Top Attack Paths](#) tab with the appropriate filter automatically applied. Here you can view paths that match the selected value.





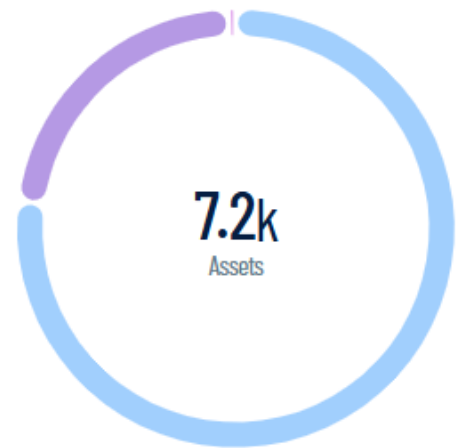
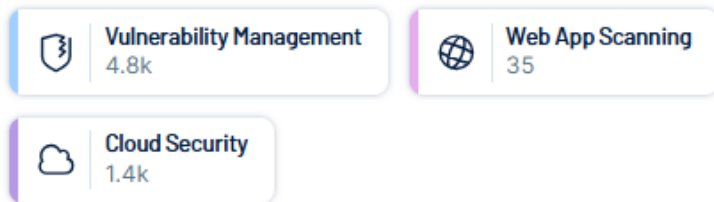
## Total Assets

The **Total Assets** section of the **Home** page shows you a snapshot of all of your active assets within Tenable Exposure Management and the exposure categories from which their data originates.

**Tip:** For more information about data sources, see [Exposure Categories](#).

### Total Assets

#### Exposure Category ⓘ



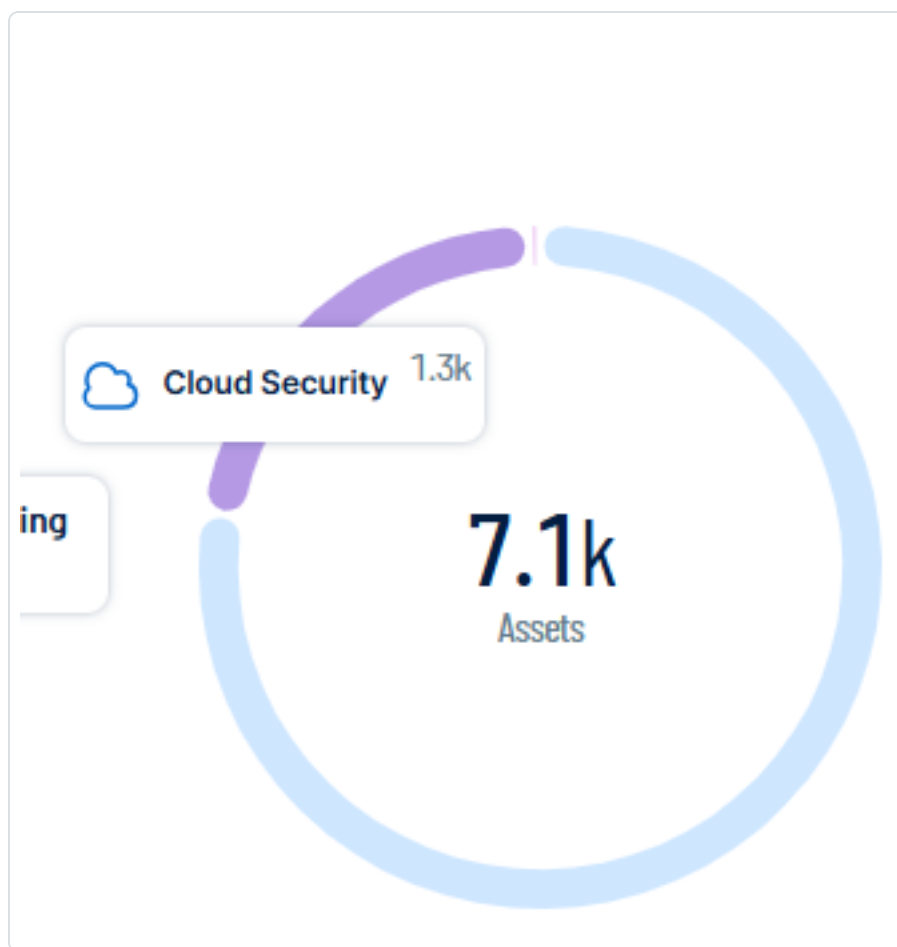
[See in Inventory](#) >

Here, you can:

- In the **Exposure Category** section, view tiles that represent each individual exposure category whose sources feeding asset data into Tenable Exposure Management.
  - Click a tile to navigate directly to the [Assets](#) page filtered by the selected exposure category.
- View a graphical representation of your total assets separated by their relevant exposure category.



- Hover your mouse over a graph segment to view additional details about that segment.



- Click **See in Inventory** to navigate directly to the [Inventory](#) page automatically filtered to display licensed, active assets.

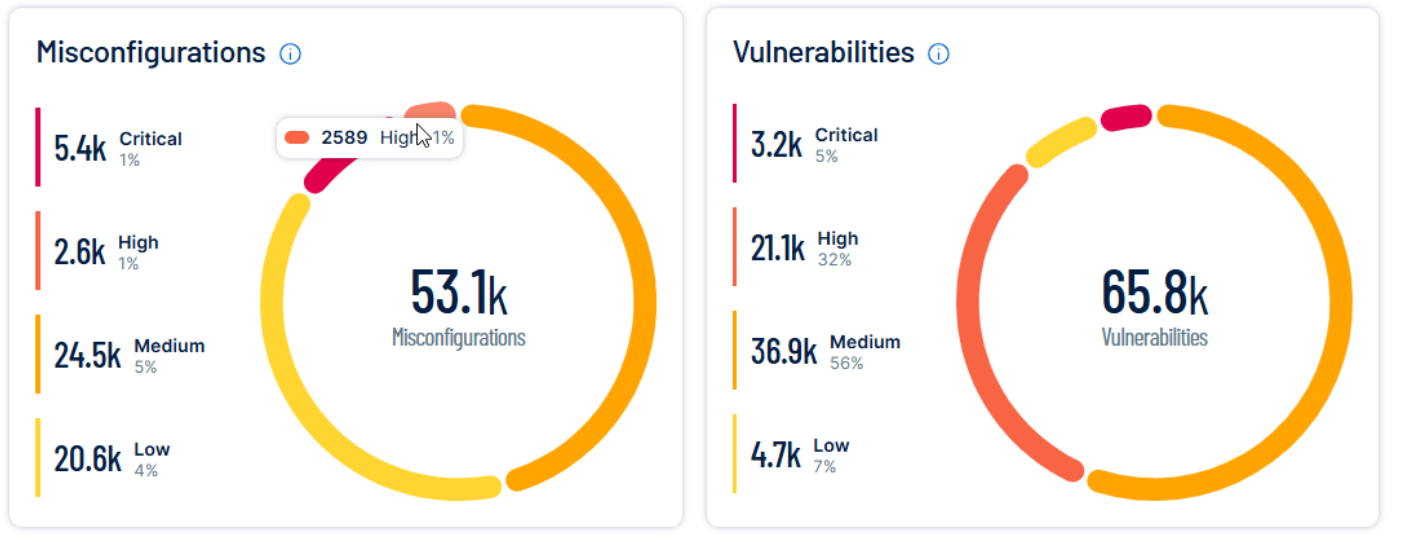
## Total Active Findings

A finding is a single instance of a weakness (vulnerability or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol. The **Total Active Findings** section of the **Home** page shows you a snapshot of the types of findings within Tenable Exposure Management and their respective severities.

**Important:** This section includes data from all findings that are not in the **Fixed** state (i.e., **Active**, **Resurfaced**, and **New** findings).



## Total Active Findings



Here, you can:

- View a tile that highlights all **Misconfigurations** among your assets:
    - On the left side of the tile, view your misconfigurations separated by [severity](#). This section displays the number of misconfigurations within each specific severity, as well as the percentage of those misconfigurations as compared to your misconfiguration total.
- Tip:** For more information about severity and Vulnerability Priority Rating, see [Tenable Exposure Management Metrics](#).
- Click a severity count to navigate directly to the [Findings](#) page filtered by misconfigurations of the selected severity.
  - View a graphical representation of your misconfigurations separated by their relevant severity.
    - Hover your mouse over a graph segment to view additional details about that segment.
- View a tile that highlights all **Vulnerabilities** among your assets:



- On the left side of the tile, view the your vulnerabilities separated by [severity](#). This section displays the number of vulnerabilities within each specific severity, as well as the percentage of those vulnerabilities as compared to your vulnerability total.

**Tip:** For more information about severity and Vulnerability Priority Rating, see [Tenable Exposure Management Metrics](#).

- Click a severity count to navigate directly to the [Findings](#) page filtered by vulnerabilities of the selected severity.
- View a graphical representation of your vulnerabilities separated by their relevant severity.
  - Hover your mouse over a graph segment to view additional details about that segment.



---

## Exposure Signals

---

An *Exposure Signal* can be defined as a combination of risks that could make any weakness potentially dangerous to your business. For example, an account with:

- Privileged access to a business-critical application
- Unpatched vulnerabilities on their device
- A device not covered by EDR

Is a candidate for an exposure signal, because these weaknesses combined on an asset makes this person a risk to their organization.

Within Tenable Exposure Management, you can generate exposure signals that use queries to search for asset *violations*. Simply put, if an asset is impacted by a weakness related to the query, then the asset is considered a *violation*. On the **Exposure Signals** page, you can view, generate, and interact with the data from queries and their impacted asset violations.

Using this, you can:

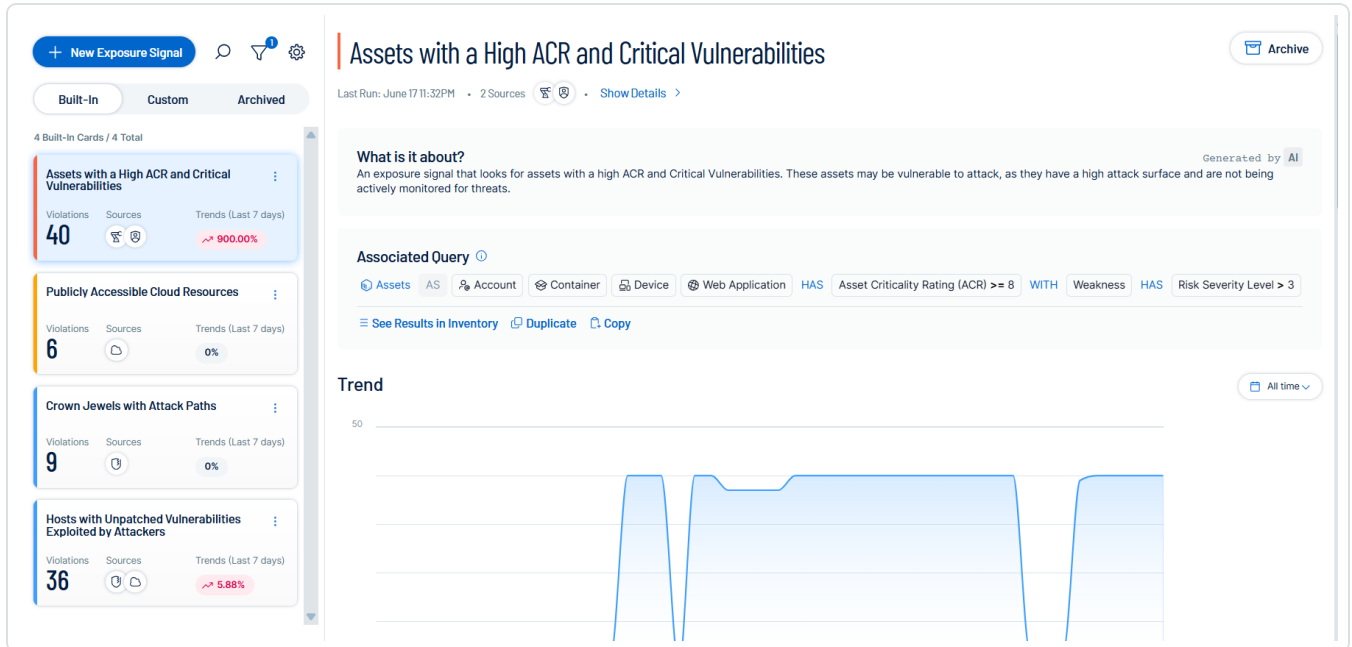
- Gain visibility into your most critical risk scenarios
- Create custom exposure signals to view business-specific risks and weaknesses

To access the **Exposure Signals** page:



1. In the left navigation menu, click **Exposure Signals**.

The **Exposure Signals** page appears.




The **Exposure Signals** page includes the following sections:

## Exposure Signals List

On the left side of the page, you can view a list of cards representing exposure signals.

You can manage the list in the following ways:


- Search the list
  1. In the upper-right corner of the list, click the  button.

The search box appears.
  2. In the search box, type the criteria by which you want to search the exposure signals list.

Tenable Exposure Management filters the list by the specified criteria.

- Filter the list



1. In the upper-right corner of the list, click the  button.


The **Filter By Sources** window appears.

2. Select the check box next to each data source by which you want to filter the exposure signals list.

Tenable Exposure Management filters the list by the specified criteria.

**Tip:** Click **Clear Filter** to remove all applied filters from the list.

- Manage the list settings

1. In the upper-right corner of the list, click the  button.

The **Settings** window appears.

2. In the **View Preferences** section, select one of the following options:

- **Show all Exposure Signals** – Show all exposure signal cards regardless of if their combinations result in a violation.
- **Show only combinations resulting in violations** – Show only exposure signal cards that include combinations resulting in a violation.

3. In the **Card Sorting** section, select one of the following options:

- **Alphabetic Order** – List exposure signal cards in alphabetical order.
- **Alphabetic Reverse** – List exposure signal cards in reverse alphabetical order.
- **Highest Violation** – List exposure signal in order of the highest violation first.
- **Lowest Violation** – List exposure signal in order of the lowest violation first.
- **Changed frequently in the last 7 days** – List only exposure signals that have been updated within the last 7 days.

4. Click **Save**.

The list includes the following tabs:



- **Built-In** – The cards in this section represent Tenable-provided exposure signals. You cannot edit built-in exposure signals.
- **Custom** – The cards in this section represent user-created custom exposure signals. To add exposure signals to this section, you can:
  - [Add a Custom Exposure Signal](#)
  - [Duplicate an Exposure Signal Query](#)
  - [Duplicate a Custom Exposure Signal](#)
- **Archive** – The cards in this section represent all exposure signal cards that have been archived.

**Tip:** To unarchive an exposure signal, in the upper-right corner of the card, click the **Unarchive** button. Tenable Exposure Management reactivates the exposure signal and moves the card to the appropriate section of the exposure signals list.


Each card includes the following information:







- **Severity** – Each card is color coded to indicate the severity associated with the exposure signals, for example:
  - Dark Red – Critical
  - Light Red – High
  - Orange – Medium
  - Yellow – Low
  - Blue – Info
- **Violations** – The number of assets found in violation of the exposure signal.
- **Sources** – The [exposure management categories](#) associated with the exposure signal.
- **Trends** – The trend and percentage of change in violations within the last 7 days. For example, if the violations for this combination have increased by 5.45%, you'd see 5.45%.

**Note:** Because data on exposure signal cards only refreshes once every 24 hours, you may notice a difference in violation counts between these cards and the rest of the Tenable Exposure Management interface, including the [Impacted Assets](#) section.





In the upper right corner of a card, click the  button to view additional options:

Tab	Menu Options
Built-In	<ul style="list-style-type: none"><li>Click  <b>Archive</b> to move the exposure signal card to the <b>Archived</b> section of the list.</li></ul>
Custom	<ul style="list-style-type: none"><li>Click  <b>Edit</b> to make changes to the exposure signal card. For more information, see <a href="#">Edit a Custom Exposure Signal</a>.</li><li>Click  <b>Duplicate</b> to make a copy of the exposure signal card. For more information, see <a href="#">Duplicate a Custom Exposure Signal</a>.</li><li>Click  <b>Archive</b> to move the exposure signal card to the <b>Archived</b> section of the list. For more information, see <a href="#">Archive a Custom Exposure Signal</a>.</li><li>Click  <b>Delete</b> to permanently delete the exposure signal card from the <b>Exposure Signals</b> page. For more information, see <a href="#">Delete a Custom Exposure Signal</a>.</li></ul>
Archive	Click  <b>Delete</b> to permanently delete the exposure signal card from the <b>Exposure Signals</b> page.

## Exposure Signal Details

When you click on a card in the [Exposure Signals](#), the details for that card appear on the right side of the page.

### Basic Information and Summary

At the top of the details section, you can view the following information:

- The name of the exposure signal.
- Last Run** — The date and time at which information was last generated for the exposure signal.
- Sources** — The number of and the icons for each [exposure management category](#) associated with the exposure signal.
- Click **Show Details** to view additional exposure signal information:



- **Exposure Signal Info** – A brief description of the exposure signal and its creator.
- **Tenable Data Sources** – The [exposure management categories](#) associated with the exposure signal.
- **(Not supported in [FedRAMP](#) environments) What is it about?** – This section displays an AI-generated summary of the exposure signal, including information about why the combination may be a risk to you.

## Associated Query

In this section, you can view the asset query that generated the exposure signal.

**Associated Query** ⓘ

Assets AS Device HAS

Sources = ( Tenable Identity Exposure, Tenable Identity Exposure (AD), Tenable Identity Exposure (Microsoft Entra ID) )

AND NOT

Sources = Tenable Vulnerability Management

[See results in Asset Inventory](#) [Duplicate](#) [Copy](#)

Below the query, you can select any of the following options:

- **See results in Asset Inventory** – Click to navigate directly to the [Assets](#) view, where you can view the asset query and the asset list filtered by the query results.
- **Duplicate** – Click to duplicate the exposure signal into a new, custom exposure signal. From here, you can manage and edit the exposure signal to fit your needs before saving it to the [Custom](#) section of the exposure signals list.
- **Copy** – Click to copy the query to your device's clipboard. You can then paste the query for use/editing in the [Global Asset Search](#), or you can save it for later.

## Trend

In the **Trend** section, you can view a graphical representation of how the number of violations within the selected exposure signal has changed over a specific period of time.



To change the period of time for which you want to view the trend, in the upper-right corner of the section, expand the drop-down menu and select one of the following options:

- **All time**
- **Last year**
- **Last quarter**
- **Last month**
- **Last 7 days**

**Tip:** Hover your mouse cursor over any point on the graph to view the exact number of violations on that date.

## Impacted Assets

In this section, you can view a list of the impacted assets (assets found in violation) of the exposure signal.



## Impacted Assets

Search				
Name	Class	Weaknesses	Sources	AES
tenable-attack-path...	Storage	S3 Bucket does not bloc... S3 Bucket is not encrypt... <a href="#">+ 3 More</a>		<div><div></div></div> 914 <a href="#">See Details &gt;</a>
dc01	Device	CVE-2024-38193 CVE-2023-35343 <a href="#">+ 1288 More</a>		<div><div></div></div> 923 <a href="#">See Details &gt;</a>

**Tip:** Use the search box to search for a specific impacted asset.

This list includes the following asset information:

- **Name** — The asset identifier. Tenable Exposure Management assigns this identifier based on the presence of certain asset attributes in the following order:
  1. Agent Name (if agent-scanned)
  2. NetBIOS Name
  3. FQDN
  4. IPv6 address
  5. IPv4 address

For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.

- **Class** — The class type associated with the asset. For more information, see [Asset Classes](#).
- **Weaknesses** — The weaknesses associated with the asset. For more information, see [Weaknesses](#).
- **AES** — The [Asset Exposure Score](#) for the asset. The AES represents the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

**Note:** Tenable Exposure Management does not calculate an ACR for unlicensed assets.

- **Click the See Details to view additional asset details:**



The asset details panel appears.



dc01

[See Asset Details](#)



### Exposure Signals Summary

Gen AI

Tenable is considering the asset "dc01" to be part of the exposure insight "Cloud Resources with Critical Severity Findings and High Exposure Score" because: it is a Device with an AES rating of 700 or higher, indicating a high level of exposure. This Device, identified as an AWS EC2 instance with the FQDN ec2-18-217-143-103.us-east-2.compute.amazonaws.com, was last observed on February 3rd, 2025 at 4:47PM UTC and has 1290 weaknesses, including critical severity vulnerabilities like CVE-2024-38193, CVE-2023-35343, CVE-2024-43516, and CVE-2023-32022. This combination of factors suggests a high risk of exploitation, making this asset a prime target for attackers.

### Key Properties (7)



Last Observed At Feb 3, 2025 11:47AM

Created Date Jan 21, 2025 4:34AM

Host Fully Qualified DNS ec2-18-217-143-103.us-east-2.c...

Device System Type aws-ec2-instance

Asset Class 

Sources 

AES 923

### Weaknesses (1290)



Search



CVE-2023-21684





This panel includes the following asset information:

Section	Information
Header	View the asset name. Below the name, click <b>See Asset Details</b> to navigate directly to the full <a href="#">Asset Details</a> page for the selected asset.
Exposure Signal Summary	<b>(Not supported in <a href="#">FedRAMP</a> environments)</b> View an AI-generated summary of the exposure signals, including information about why the combination may be a risk to you.
Key Properties	<p>View high-level <b>Key Properties</b>, including:</p> <ul style="list-style-type: none"><li>◦ <b>Last Observed At</b> – The date and time at which a scan most recently identified the asset.</li><li>◦ <b>Created Date</b> – The date and time at which the asset record was created in Tenable Exposure Management.</li><li>◦ <b>Host Fully Qualified DNS</b> – The Host Fully Qualified Domain Names, or FQDNs, of the asset host.</li><li>◦ <b>Device System Type</b> – The type associated with the asset's device system, for example, <b>plc</b>.</li><li>◦ <b>Asset Class</b> – The <a href="#">asset class</a> associated with the asset, for example, <b>Device</b>.</li><li>◦ <b>ACR</b> – The <a href="#">Asset Criticality Rating</a> for the asset. The ACR represents the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.</li></ul>
Weaknesses	<p>View a list of all weaknesses associated with the asset. Click on a weakness to navigate directly to the <a href="#">Weakness Details</a> page for the selected weakness.</p> <div><b>Tip:</b> Use the search box to search for a specific weakness on the asset.</div>

## Manage Exposure Signals



On the [Exposure Signals](#) page, you can manage built-in and create custom exposure signals to view specific risks and weaknesses that relate to your business and its needs. You can fine-tune these combinations to quickly highlight the information that's most important to you.

You can add and manage your exposure signals in the following ways:

### Add a Custom Exposure Signal

To add a custom exposure signal:

1. Access the [Exposure Signals](#) page.
2. Do one of the following:
  - To create a custom exposure signal based on an existing combination, select the card from the [Exposure Signals List](#) and, in the [Associated Query](#) section, click **Duplicate**.
  - To create a new custom exposure signal, at the top of the [Exposure Signals List](#), click **+** **New Exposure Signal**.

The **New Exposure Signal** page appears.

Name	ACR	Class	Last Observed At	Created Date	Host Fully Qualified D...	Device System Type
tenable icp #36	7	Device	May 19, 2025 3:14AM	May 19, 2025 3:14AM		tenable icp
tenable em #31	7	Device	May 23, 2025 5:56PM	May 23, 2025 5:56PM		tenable em
tenable icp #100	7	Device	May 26, 2025 5:14AM	May 22, 2025 6:24AM		tenable icp
tenable icp #131	7	Device	May 25, 2025 4:48PM	May 25, 2025 4:48PM		tenable icp
ot server #19	9	Device	May 27, 2025 8:51AM	May 22, 2025 4:12AM		ot server
tenable icp #147	7	Device	May 26, 2025 9:31AM	May 26, 2025 9:31AM		tenable icp
endpoint #318	7	Device	May 26, 2025 7:51AM	May 25, 2025 1:02PM		endpoint
tenable icp #99	7	Device	May 26, 2025 4:56AM	May 22, 2025 5:24AM		tenable icp
tenable em #45	7	Device	May 26, 2025 3:52AM	May 26, 2025 3:52AM		tenable em
endpoint #278	7	Device	May 20, 2025 8:45PM	May 20, 2025 8:45PM		endpoint

3. In the **Query builder** section, build the query you want to use for the exposure signal:

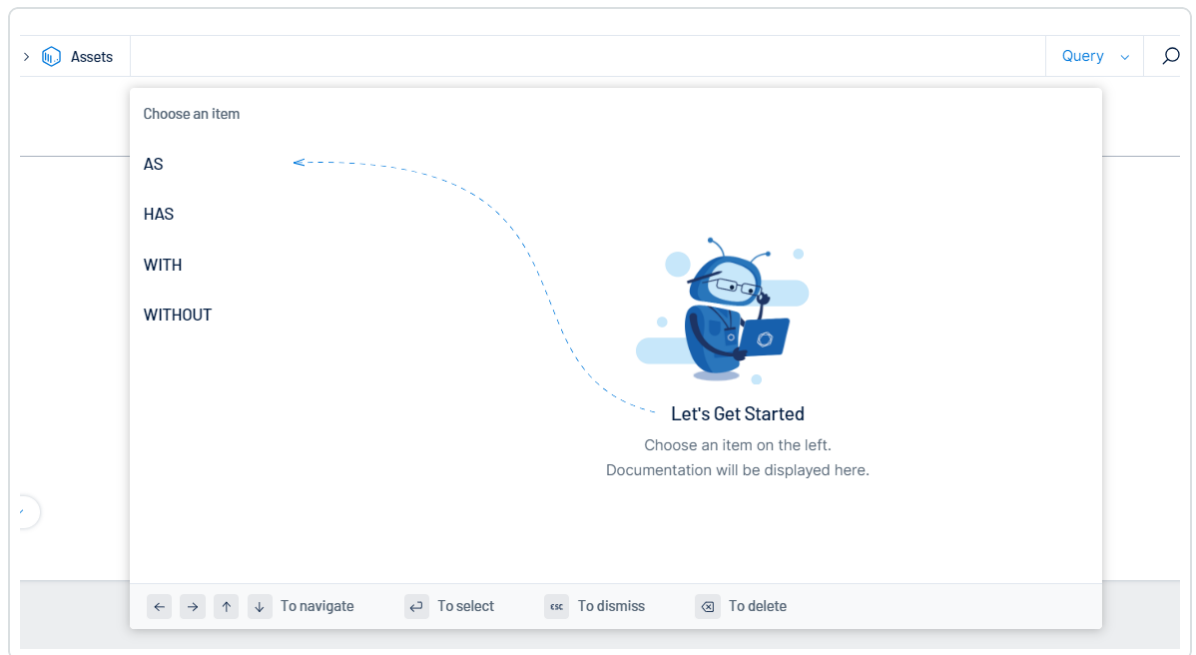
#### Build a query string:

- a. On the right side of the global search bar, in the drop-down, select **Query**.
- b. Click inside the **Search for Assets** text box.





The search query builder appears.



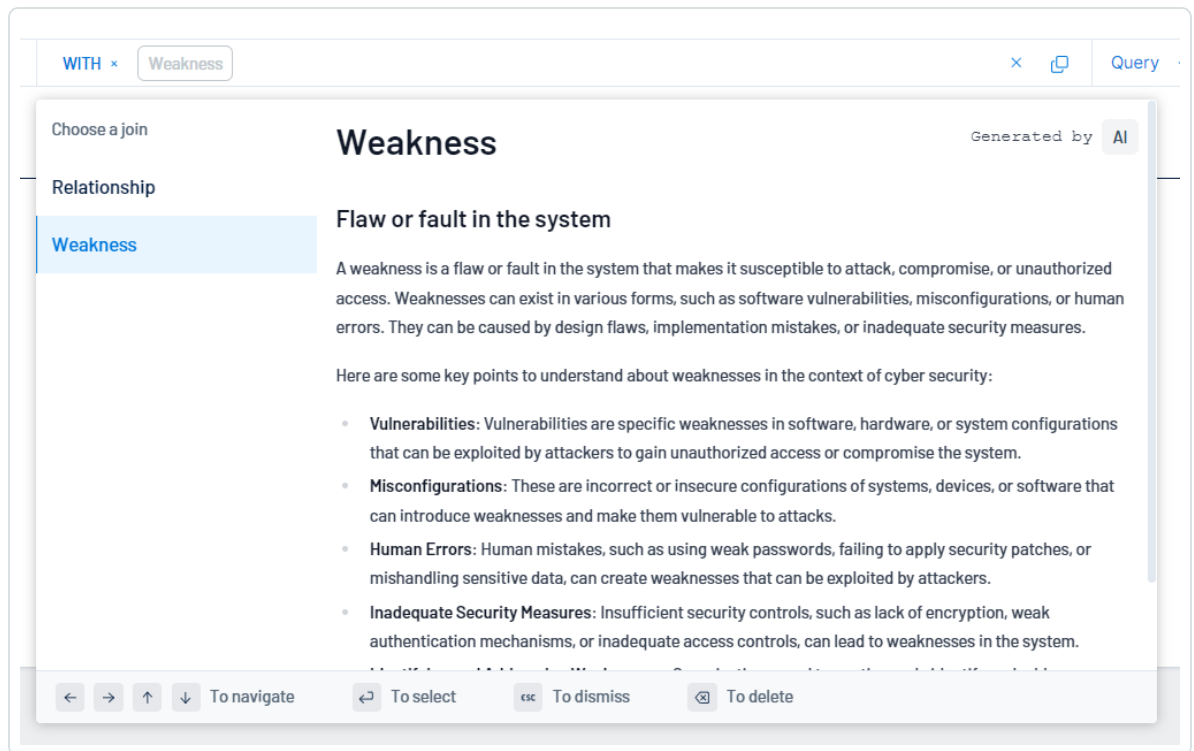
**Tip:** You can also build your query using your keyboard. Follow the instructions on the bottom of the query builder to navigate.

- c. On the left side of the query builder, choose an operator to begin your search.

**(Not supported in [FedRAMP environments](#))** Hover your mouse cursor over an item to view an AI-generated description of how the operator filters your assets.

- d. Select a qualifier for your query.

**(Not supported in [FedRAMP environments](#))** Hover your mouse cursor over an item to view an AI-generated description of how the item filters your assets.



**Note:** Tenable Exposure Management only displays qualifiers and operators that generate a working query. You cannot select items that break the query string.

- e. (Optional) Where applicable, add additional items and qualifiers to the query.

**Tip:** Click on a query token to edit that section of the query without starting over!

- f. On the right side of the search bar, click the  button.

Tenable Exposure Management performs the search and filters the asset list based on your query.

#### • Build a query based on Natural Language Processing:

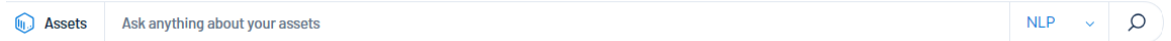
The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

You can use Natural Language Processing (NLP) to ask questions about your assets and receive an AI-generated list.



- a. On the right side of the global search bar, in the drop-down, select **NLP**.
- b. In the **Ask anything about your assets** text box, type a question you want to ask about your assets. For example, you could ask *"Which critical devices do I have that are connected to the internet?"*.

**Tip:** For more suggestions on questions to ask based on your business context, see [NLP Search Use Cases](#).




Tenable Exposure Management performs a search and provides an AI-generated list of assets that match the query. If no data is available, an error message appears indicating no data could be generated for the search criteria you entered.

4. In the **Name** text box, type a name for the exposure signal.
5. From the **Priority** drop-down, select the priority you want to assign to the exposure signal, for example, **High**.
6. In the **Description** text box, type a description for the exposure signal.
7. Click **Save Exposure Signal**. Tenable Exposure Management saves the exposure signal and adds a new card to the [Custom](#) tab of the exposure signals list.

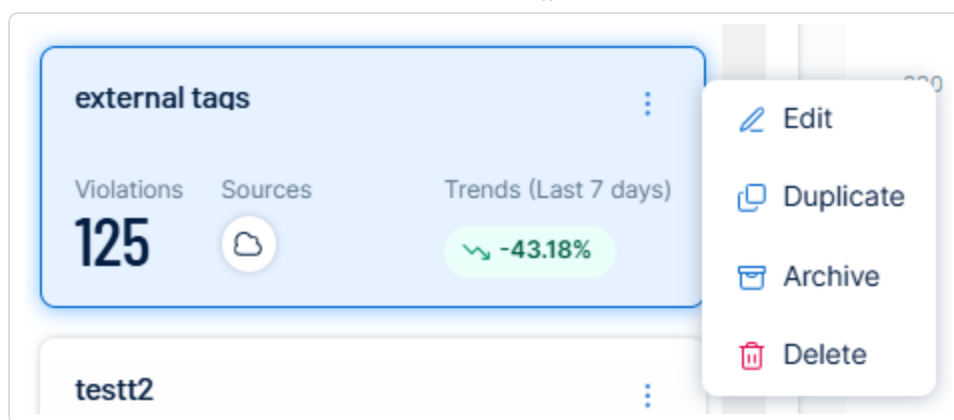
### Edit a Custom Exposure Signal


**Note:** You cannot edit Tenable-provided exposure signals.

To edit a custom exposure signal:

1. Do one of the following:
  - On the [Custom](#) tab of the exposure signals list, on the card for the exposure signal you want to edit, click the  button.

Menu options appear.



a. In the menu, click  **Edit**.

- On the [Custom](#) tab of the exposure signals list, click on the card for the exposure signal you want to edit.

The [Exposure Signal Details](#) for that card appear.

a. In the upper-right corner of the page, click  **Edit**.


The **Edit Exposure Signal** page appears.

2. Make any desired changes to the exposure signal.
3. Click **Save**. Tenable Exposure Management saves your changes to the exposure signal.

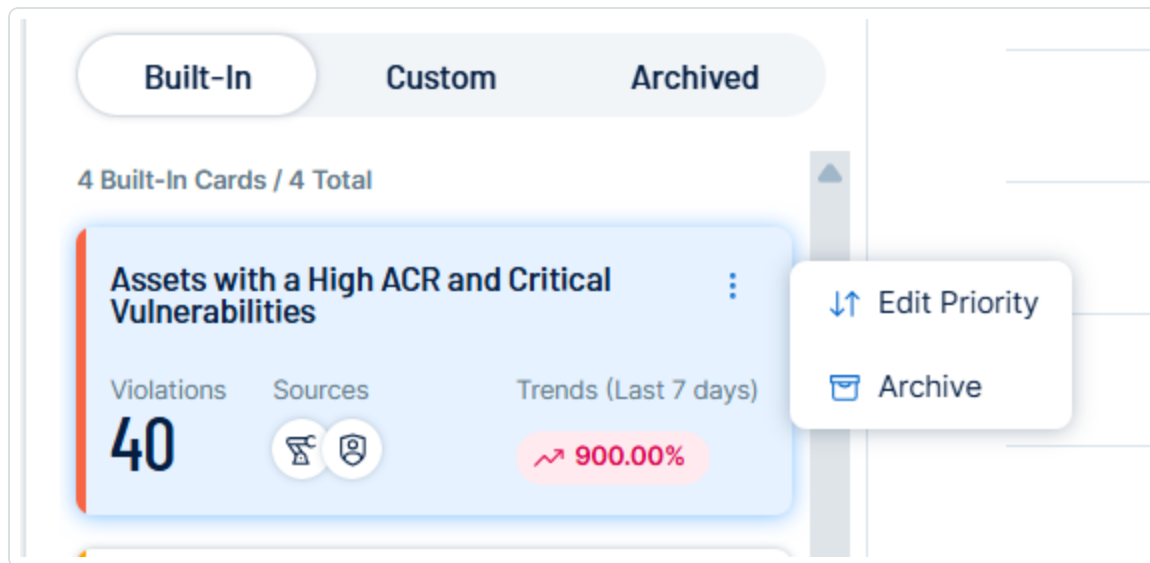
## Edit the Priority of a Built-In Exposure Signal

**Note:** You can only edit the priority of Tenable-provided exposure signals.

To edit the priority of a built-in exposure signal:

1. On the [Built-In](#) tab of the exposure signals list, on the card for the exposure signal you want to edit, click the  button.

Menu options appear.



2. In the menu, click ↓↑ **Edit Priority**.

The **Edit Priority** window appears.

**Edit Priority** ×

"Assets with a High ACR and Critical Vulnerabilities"

[Reset to Tenable Default](#)

Info Low Medium **High** Critical

**\* Override Reason**

Specify Override Reason

[Cancel](#) [Save](#)

3. Click and drag the slider to the priority you want to apply to the exposure signal.
4. In the **Override Reason** text box, type the reason for overriding the Tenable-reported priority for the exposure signal.
5. Click **Save**. Tenable Exposure Management saves your changes to the exposure signal priority.

### Duplicate a Custom Exposure Signal

You can duplicate a exposure signal to use it as a template to create a new custom exposure signal.

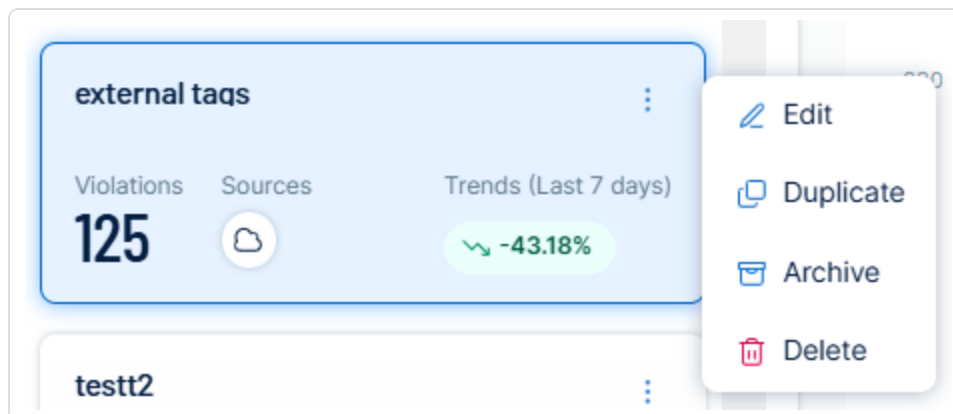
**Tip:** To duplicate a Tenable-provided exposure signal, [duplicate](#) the exposure signal's [associated query](#).



To duplicate a custom exposure signal:

1. On the **Custom** tab of the exposure signals list, on the card for the exposure signal you want to duplicate, click the **⋮** button.

Menu options appear.



2. In the menu, click **Duplicate**.

The **New Exposure Signal** page appears.

3. Follow the steps to [add a new custom exposure signal](#).

## Archive a Custom Exposure Signal

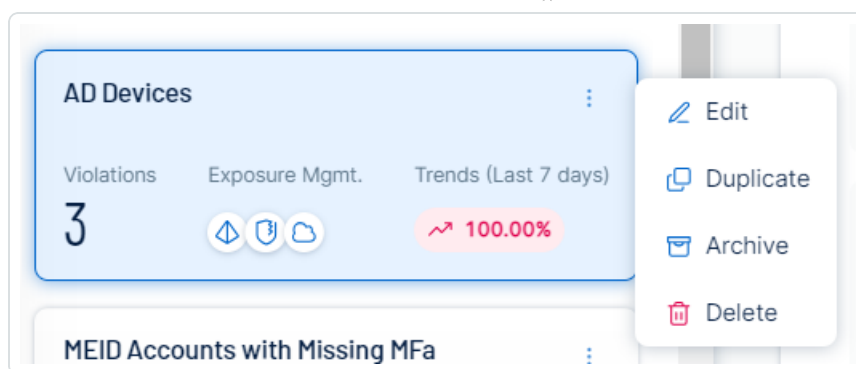
When you archive a exposure signal, Tenable Exposure Management moves that exposure signal card to the **Archived** section of the exposure signal list. When you archive an exposure signal, the historical data for that combination is permanently deleted and cannot be retrieved.

**Tip:** You can also archive Tenable-provided exposure signal cards.

To archive a exposure signal:

1. Do one of the following:
  - On the **Custom** tab of the exposure signals list, on the card for the exposure signal you want to archive, click the **⋮** button.

Menu options appear.



a. In the menu, click  **Archive**.

- On the **Custom** tab of the exposure signals list, click on the card for the exposure signal you want to archive.

The [Exposure Signal Details](#) for that card appear.

a. In the upper-right corner of the page, click  **Archive**.

A confirmation message appears.

2. Click **Archive**.

Tenable Exposure Management moves the exposure signal card to the **Archived** section of the [Exposure Signals List](#).

**Tip:** To unarchive a exposure signal, in the upper-right corner of the card, click the **Unarchive** button. Tenable Exposure Management reactivates the exposure signal and moves the card to the appropriate section of the exposure signals list.

## Delete a Custom Exposure Signal

You can permanently delete custom exposure signal cards from the Tenable Exposure Management interface. When you delete a exposure signal, all data for that card, including queries and historical results, are permanently deleted and cannot be retrieved.



**Note:** You cannot delete built-in exposure signal cards.

To delete a custom exposure signal:

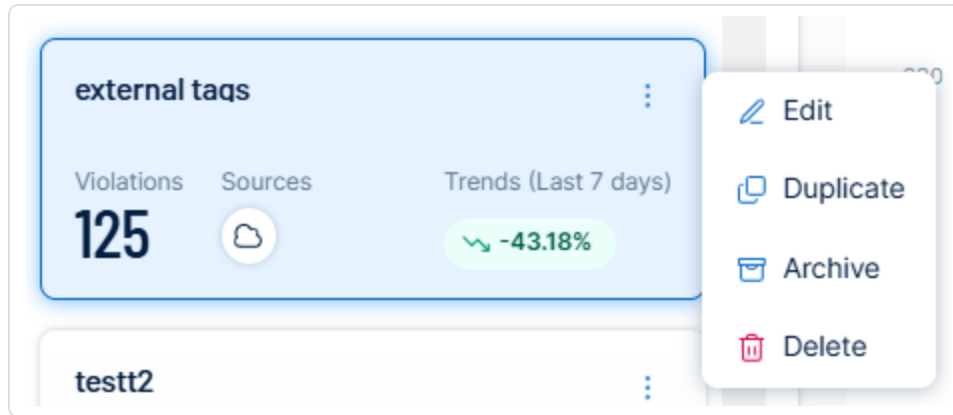




1. Do one of the following:

- To delete an active exposure signal, on the [Custom](#) tab of the exposure signals list, on the card for the exposure signal you want to delete, click the  button.
- To delete an archived exposure signal, on the [Archived](#) tab of the exposure signals list, on the card for the exposure signal you want to delete, click the  button.

Menu options appear.



2. In the menu, click  **Delete**.

A confirmation message appears.

3. Click **Delete Exposure Signal**.

Tenable Exposure Management permanently deletes the exposure signal and all of its associated data from the application.



---

# Inventory

---

The **Inventory** page in Tenable Exposure Management aggregates all assets and their associated entities to unify and operationalize the data. It focuses on your organization's ability to maintain an accurate inventory of all of your cyber-enabled technologies, while providing data analytics and a comprehensive inventory across various sources. While asset management highlights processes and people that can be affected, Tenable Exposure Management takes this one step further by digging into the technologies that can be hacked and allowing you to gain insight into these exposures.

Simply put, the **Inventory** page is the central repository of all cyber assets across an organization's attack surface by providing:

- A comprehensive list of all digital assets
- A complete view of risks using enriched context
- Built-in control, monitoring, and alerting
- Unified asset analysis to drive prioritization

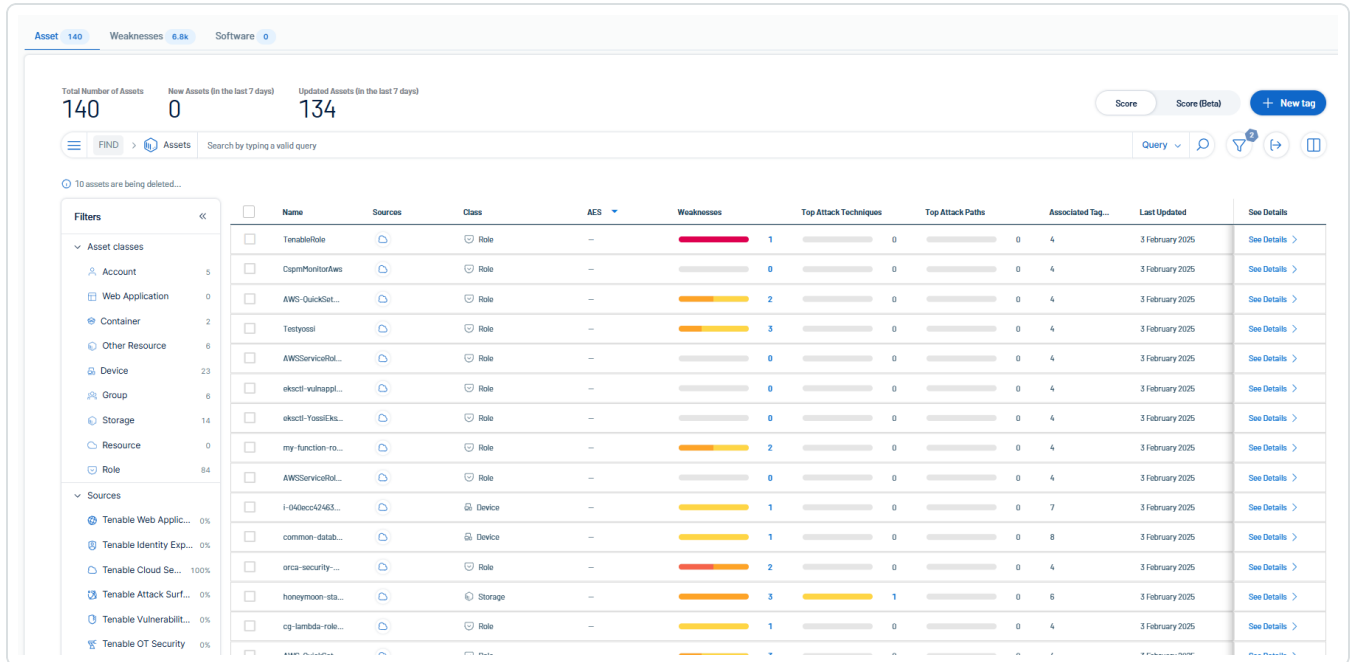
Tenable Exposure Management aids prioritization by highlighting the following asset data:

- Centralized location
- Asset class breakdown
- Filters
- Related weaknesses

To access the Inventory page:

1. In the left navigation menu, click **Inventory**.

The **Inventory** page appears with the **Assets** tab displayed by default.



On the **Inventory** page, you can:

- View and interact with the data on the [Assets](#) tab.
- View and interact with the data on the [Weaknesses](#) tab.
- View and interact with the data on the [Findings](#) tab.
- View and interact with the data on the [Software](#) tab.

## Assets

The **Assets** tab on the **Inventory** page allows you to view and manage all of your assets. You can quickly see which assets are new or updated, which class the asset belongs to, and other useful asset information.

**Important:** Because they do not include a hardware ID attribute, Microsoft Entra ID devices managed by Microsoft Intune's mobile device management (MDM) are not visible on the Tenable Exposure Management **Assets** tab.

To access the **Assets** tab:



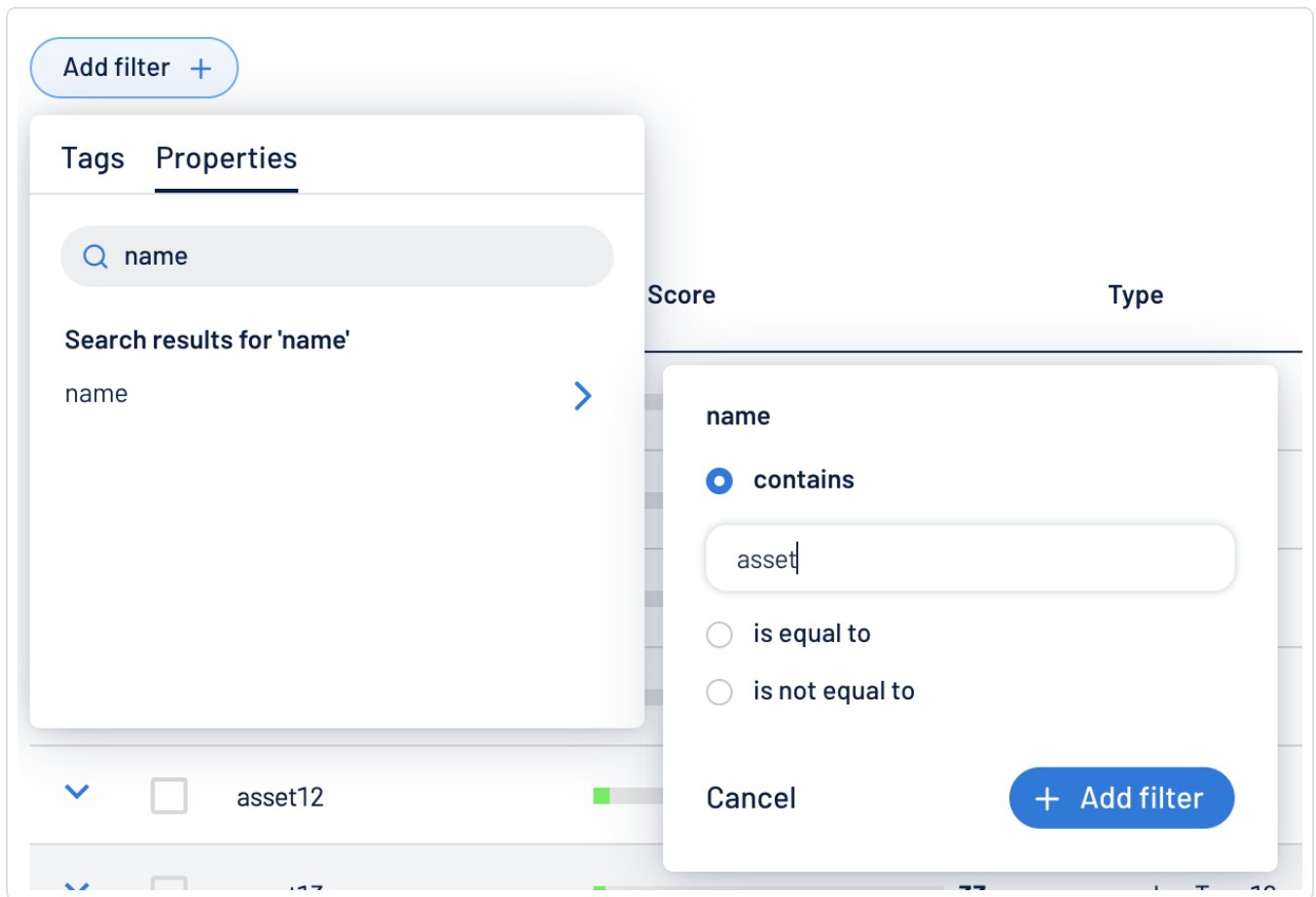
1. Access the [Inventory](#) page.

The **Assets** tab appears by default.

Asset Name	Sources	Asset Class	AES	Active Finding Count	Associated Tags Count	Last Update Date	See Details
jenkins-aws	Wiz	Device	991	58	4	22 July 2025	See Details
redhat-customer-rela...	Wiz	Device	985	40	4	22 July 2025	See Details
redhat-customer-rela...	Wiz	Device	985	40	4	22 July 2025	See Details
xz-utils-danil	Wiz	Device	984	26	4	21 July 2025	See Details
models-backup-trainl...	Wiz	Device	982	26	5	21 July 2025	See Details
teamCity_critical_danil	Wiz	Device	980	28	4	21 July 2025	See Details
leaky-wizard	Wiz	Device	980	30	4	22 July 2025	See Details
Wiz_Fortinet	Wiz	Device	978	24	4	22 July 2025	See Details
prod-webserv-misco...	Wiz	Device	978	24	5	21 July 2025	See Details
ssm-machine-test	Wiz	Device	978	21	4	22 July 2025	See Details
jd-malware-test	Wiz	Device	978	22	4	22 July 2025	See Details
trigger	Wiz	Device	978	24	5	22 July 2025	See Details

On the **Assets** tab, you can:

- View the **Total Number of Assets** within your container.
- View the total number of **New Assets** discovered within the last 7 days.
- View the total number of Updated Assets within your container in the last 7 days.
- Use the search box above the asset list to search for a specific asset in the list. For more information, see [Global Asset Search](#).
- Filter the asset list:



a. Click the  button.

The **Add filter**  button appears.

b. Click **Add filter** .

A menu appears.

c. Do one of the following:

- To search the asset list by tag, click **Tags**.
- To search the asset list by asset property, click **Properties**.

**Tip:** See [Asset Filters](#) for additional information on available filter types.


d. In the search box, type the criteria by which you want to search the asset list.



Tenable Exposure Management populates a list of options based on your criteria.

- e. Click the tag or property by which you want to filter the asset list.

A menu appears.


- f. Select how to apply the filter. For example, if you want to search for an asset whose name is *Asset14*, then select the **contains** radio button and in the text box, type *Asset14*.
- g. Click **Add filter** .

The filter appears above the asset list.

- h. Repeat these steps for each additional filter you want to apply.
- i. Click **Apply filters**.

Tenable Exposure Management filters the asset list by the designated criteria.

- Export the table or the page:

- a. (Optional) To export only specific table rows, in the table, select the check box next to the rows you want to export.
- b. Click the  button.

The **Export** window appears.



## Export



### General

☐ Entire Table ☐ Current Page ☒ Selected Rows (3)

### File Name

Enter a name for the exported file.

### Formats

☒ CSV

☐ JSON

### Columns

Search columns

☒ 9 of 9 fields selected

[View selected](#)

☒ AES

☒ Asset Class

☒ Asset Name

☒ Associated Tags Count

☒ Last Update Date

Cancel

Export



c. Do one of the following:

- To export the entire table, select the **Entire Table** radio button.

**Note:** When you export the entire table, Tenable Exposure Management only includes the first 50 columns. To view asset data for a larger number of assets, use the [Search Assets API](#) call.

- To export the current page, select the **Current Page** radio button.
- To export the selected rows, select the **Selected Rows** radio button.

d. In the **File Name** text box, type a file name to give the exported file.

e. In the **Formats** section, select the format in which you want to export the data.

f. In the **Columns** section, select the check box for each column you want to include in the export file.

g. Click **Export**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.


- Customize the columns in the table:

a. Click the  button.

The **Customize columns** window appears.

b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.

c. (Optional) In the **Show/Hide** section, select/deselect the check boxes to show or hide columns in the table.

d. (Optional) In the **Remove** section, click the  button to permanently remove a column from the table.

e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.





- i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

- ii. Select the check box next to any column or columns you want to add to the table.

- iii. Click **Add**.

The column appears in the **Customize columns** window.

- f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

- g. Click  **Apply Columns**.

Tenable Exposure Management saves your changes to the columns in the table.

- To create a [Tag](#) based on the asset list, click **+ Create**.

#### A menu appears.

- a. Click **Tag**.

You navigate directly to the [Create New Tag](#) page. By default, the tag type is set to **Dynamic**.

**Tip:** For more information, see [Tag Format and Application](#).

- To create an [Exposure Signal](#) based on the asset list, above the list, click **+ Create**.

#### A menu appears.

- a. Click **Exposure Signal**.

You navigate directly to the [New Exposure Signal](#) page.

- To the right of the asset list, in the **Filters** section, use quick filters to sort the asset list by:
  - **Sources** – Filter the asset list by the selected [data source](#).
  - **Asset classes** – Filter the asset list by the selected [asset class](#).

**Tip:** Use the search box to search for a specific source or class. Click the result to automatically filter the list by the selection.
















- View a list of your assets, including the following information:
  - **Name** – The asset identifier. Tenable Exposure Management assigns this identifier based on the presence of certain asset attributes in the following order:
    1. Agent Name (if agent-scanned)
    2. NetBIOS Name
    3. FQDN
    4. IPv6 address
    5. IPv4 address


For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.

- **Sources** – The [data source](#) from which the asset originates.



**Tip:** If there are several sources associated with the asset, you can click the **+** button to view the full list of sources.

<input type="checkbox"/>	dc.tenboneres...	 		947
<input type="checkbox"/>	apadc	  <b>+1</b>		947
<input type="checkbox"/>	dcl	  <b>+1</b>		947
<input type="checkbox"/>	rdcl			945
<input type="checkbox"/>	eks-f8c50ee4-...			927

**Tenable (1)**

-  Vulnerability Management

**3rd Party (2)**

-  Microsoft Defender
-  SentinelOne Singularity

- **Class** – The [class](#) type associated with the asset.
- **AES** – The [Asset Exposure Score](#) for the asset. The AES represents the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

**Note:** Tenable Exposure Management does not calculate an AES for unlicensed assets.

- **Active Finding Count** – The number of active [findings](#) associated with the asset.



**Important:** This count includes all findings that are not in the **Fixed** state (i.e., **Active**, **Resurfaced**, and **New** findings).

**Tip:** Click on a finding count to navigate directly to the **Findings** tab.

- **Top Attack Techniques** — Instances of attack techniques associated with this asset that are used in attack paths leading to critical assets. For more information, see [Top Attack Techniques](#).

**Tip:** Click on a count to navigate directly to the [Top Attack Techniques](#) page filtered automatically by attack path techniques related to the asset.

- **Top Attack Paths** — Attack paths related to the asset that also lead to critical assets. For more information, see [Top Attack Paths](#).

**Tip:** You can sort by this column to view which assets lead to the greatest number of attack paths.

**Tip:** Click on an attack path count to navigate directly to the [Top Attack Paths](#) page, where the **Top Attack Paths** table is automatically filtered by attack paths that feature the asset.

- **Associated tags** — The number of tags applied to the asset. For more information on tagging an asset, see [Tag Assets via the Assets Page](#).
- **Last updated** — The date and time at which the asset was last updated.
- Click **See details** to view more details about an asset. For more information, see [Asset Details](#).

## Asset Classes

Classes are how Tenable Exposure Management groups assets. Because each asset has a different business purpose, classes allow you to easily separate asset data based on its type to get the most out of your analytics.

The asset class types used in Tenable Exposure Management are as follows:

Class	Description
-------	-------------



All Assets	All assets from all sources, including third-party.
Account	The Identity login account for a software resource.
Container	Container image (e.g., Docker images).
Device	<p>Computing devices with a network stack (i.e., IP address) that could, theoretically, be a target of a Nessus scan, including the following:</p> <ul style="list-style-type: none"><li>• Traditional VM/Tenable Vulnerability Management hosts</li><li>• Active Directory "computer" object classes</li><li>• Cloud runtimes instances, such as EC2 instances</li><li>• OT devices</li><li>• ASM</li></ul> <p>For more information about how devices are profiled, see the <a href="#">Tenable One Device Profiling Quick Reference Guide</a>.</p>
Group	A grouping of persons or other groups.
Infrastructure As Code	Infrastructure as Code (e.g., Terraform, Cloud Formation).
Other Resource	General computing resources. This is a general class for all resources, including cloud runtime resources and non-host, non-identity AD assets.
Resource	An entity that an identity, Group, or Role has permissions to.
Role	Target for permissions that can be granted to persons and groups.
Storage	Cloud storage services, including AWS S3, Azure Blobs, and GCP Storage Bucket.
Web Application	Customer applications exposed on the internet .

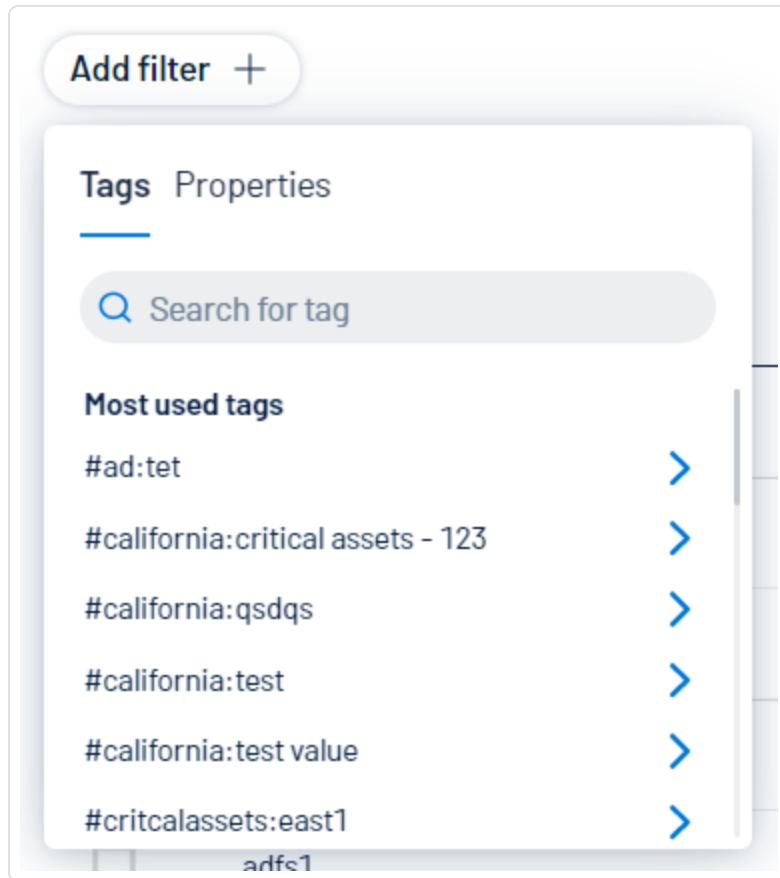
## Asset Filters

On the [Assets](#) page, you can refine the asset list using [Tag Filters](#) and [Tenable-Provided Filters](#) based on attribute properties.



## Tag Filters

[Tags](#) allow you to add descriptive metadata to assets that helps you group assets by business context. You can use tags to filter the asset list. Under the **Tags** tab, search for or select the tag by which you want to filter the list.



## Tenable-Provided Filters

Under the **Properties** tab, you can use Tenable-Provided filters to refine the asset list by the following asset properties. The following table lists some, but not all, available filters:

**Note:** The available Tenable-provided filters depend on the data sources you have configured within Tenable Exposure Management. For more information, see [Data Sources](#).

Filter	Description
id	The asset's UUID.



name	<p>The asset identifier. Tenable Exposure Management assigns this identifier based on the presence of certain asset attributes in the following order:</p> <ol style="list-style-type: none"><li>1. Agent Name (if agent-scanned)</li><li>2. NetBIOS Name</li><li>3. FQDN</li><li>4. IPv6 address</li><li>5. IPv4 address</li></ol> <p>For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the asset name.</p>
aes_score	(Requires Tenable Lumin license) The <a href="#">Asset Exposure Score (AES)</a> calculated for the asset.
last_update	The time and date when the asset record was last updated.
total_tags	The total number of tags associated with the asset.
type	The type of asset.
system_type	The system types as reported by Plugin ID 54615. For more information, see <a href="#">Tenable Plugins</a> .
created	The time and date when Tenable Exposure Management created the asset record.
sources	The source of the scan that identified the asset.
last_licensed_scan_time	The time and date of the last scan that identified the asset as licensed.
first_observed	The date and time when a scan first identified the asset.
last_observed	The date and time of the scan that most recently identified the asset.



bios_id	The NetBIOS ID for the asset.
fqdns	The fully-qualified domain name of the host that the vulnerability was detected on.
mac_addresses	A MAC address that a scan has associated with the asset record.
host_name	The hostname of the asset. This string is determined by information reported by target plugins, and is dependent on the user's environment and configuration.
netbios_name	The NetBIOS name for the asset.
network_id	The ID of the network object associated with scanners that identified the asset.
operating_systems	The operating systems that a scan identified as installed on the asset.
ssh_fingerprint	The SSH fingerprint associated with the asset.
installed_software	The software that a scan identified as installed on the asset.
acr_score	(Requires Tenable Lumin license) The asset's <a href="#">ACR</a> .
critical_vuln_counts	The number of vulnerabilities that are of critical severity on the asset.
high_vuln_counts	The number of vulnerabilities that are of high severity on the asset.
medium_vuln_counts	The number of vulnerabilities that are of medium severity on the asset.
low_vuln_counts	The number of vulnerabilities that are of low severity on the asset.
has_severity_vulns	Specifies whether the asset has associated severity vulnerabilities.



has_plugin_results	Specifies whether the has plugin results.
tenable_id	The UUID of the asset in Tenable Vulnerability Management.
service_now_sys_id	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the <a href="#">ServiceNow</a> documentation.
ipv4_addresses	<p>The IPv4 address associated with the asset record.</p> <p>This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255).</p> <div><b>Note:</b> Ensure the filter value does not end in a period.</div>
ipv6_addresses	<p>An IPv6 address that a scan has associated with the asset record.</p> <p>This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0).</p> <div><b>Note:</b> Ensure the filter value does not end in a period.</div>
last_authenticated_scan_time	The date and time of the last authenticated scan run against the asset.
cloud_source	The cloud source of the scan that identified the asset.
is_public	<p>Specifies whether the asset is available on a public network.</p> <div><b>Note:</b> A public asset is within the public IP space and identified by the <code>is_public</code> attribute in the Tenable Vulnerability Management query namespace.</div>
is_licensed	Specifies whether or not the asset is included in your license count.





aws_ec2_instance_ami_id	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_availability_zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Availability Zones in the AWS documentation.
aws_ec2_instance_id	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_ec2_instance_type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
aws_ec2_name	The name of the virtual machine instance in Amazon EC2.
aws_owner_id	A UUID for the Amazon Web Service (AWS) account that created the virtual machine instance. For more information, see AWS Account Identifiers in the AWS documentation.
aws_ec2_product_code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
aws_region	The region where AWS hosts the virtual machine instance, for example, us-east-1. For more information, see Regions and Availability Zones in the AWS documentation.
aws_ec2_instance_group_names	The group names within the virtual machine instance in Amazon EC2.
aws_ec2_instance_state_name	The state name of the virtual machine instance in AWS at the time of the scan. For possible values, see API Instance State in the Amazon Elastic Compute Cloud Documentation.
aws_subnet_id	The unique identifier of the AWS subnet where the virtual



	machine instance was running at the time of the scan.
aws_vpc_id	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.
is_managed_by_ssm	Specifies whether the asset is on a system managed by an AWS Systems Manager (SSM).
azure_resource_id	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_vm_id	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.
azure_subscription_id	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_resource_group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_location	The location of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_type	The type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
account_id	The account ID associated with the asset.
resource_name	The resource name for the asset.
resource_id	The resource ID for the asset.
resource_type	The asset's cloud resource type (for example, network, virtual



	machine).
unique_identifier	The UUID for the cloud resource account associated with the asset.
source	The source of the scan that identified the asset
region	The cloud region where the asset runs.
zone	The zone where the asset runs.
discovery_information	Specific information about how or where a scan discovered the asset.
cloud_tags	Tenable Vulnerability Management tags associated with the asset. For more information, see <a href="#">Tags</a> in the <i>Tenable Vulnerability Management User Guide</i> .
gcp_instance_id	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
gcp_project_id	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see <i>Creating and Managing Projects</i> in the GCP documentation.
gcp_zone	The zone where the virtual machine instance runs in GCP. For more information, see <i>Regions and Zones</i> in the GCP documentation.
ssl_tls_enabled	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.

## Global Asset Search

In the [Assets](#) view, you can use the global search bar to search all assets across Tenable Exposure Management. You can set up the query in any way to parse both asset and weakness data to gain the most valuable insight into your vulnerabilities.

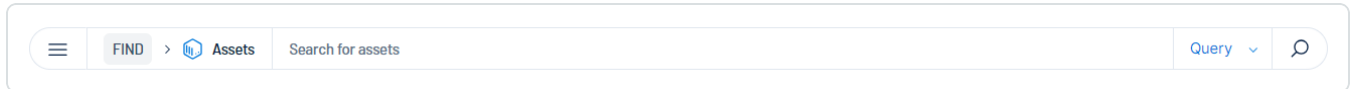
**Tip:** For additional information and examples on how to use the global asset search, see the [Global Asset Search Quick Reference Guide](#).



To use the global search:

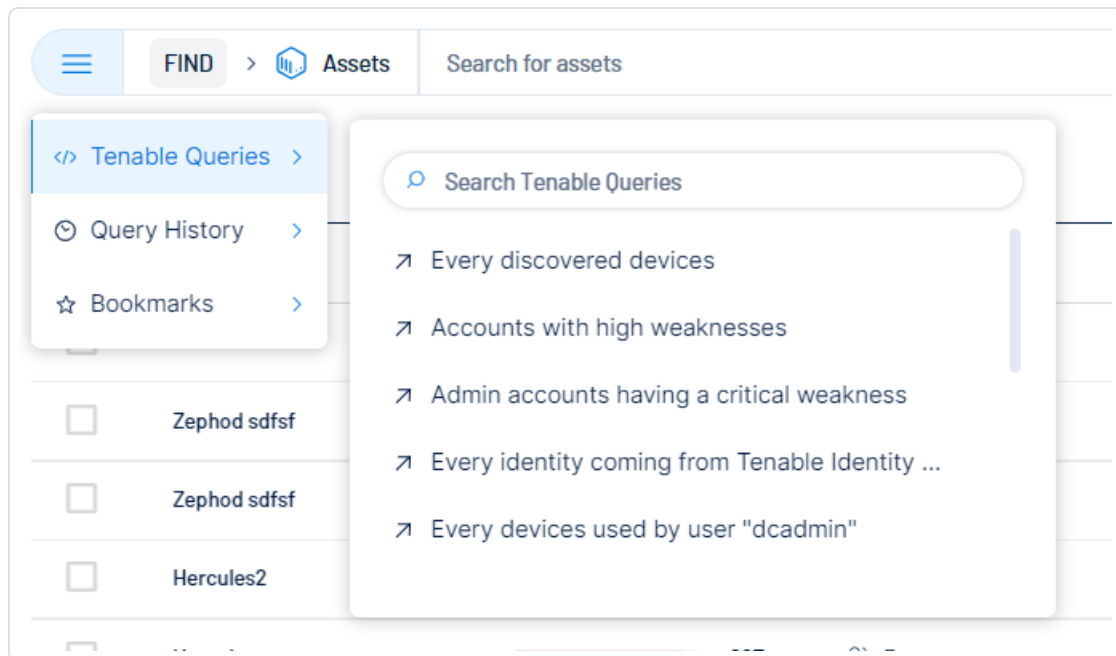
1. Access the [Assets](#) view.

At the top of the page, the global search bar appears.



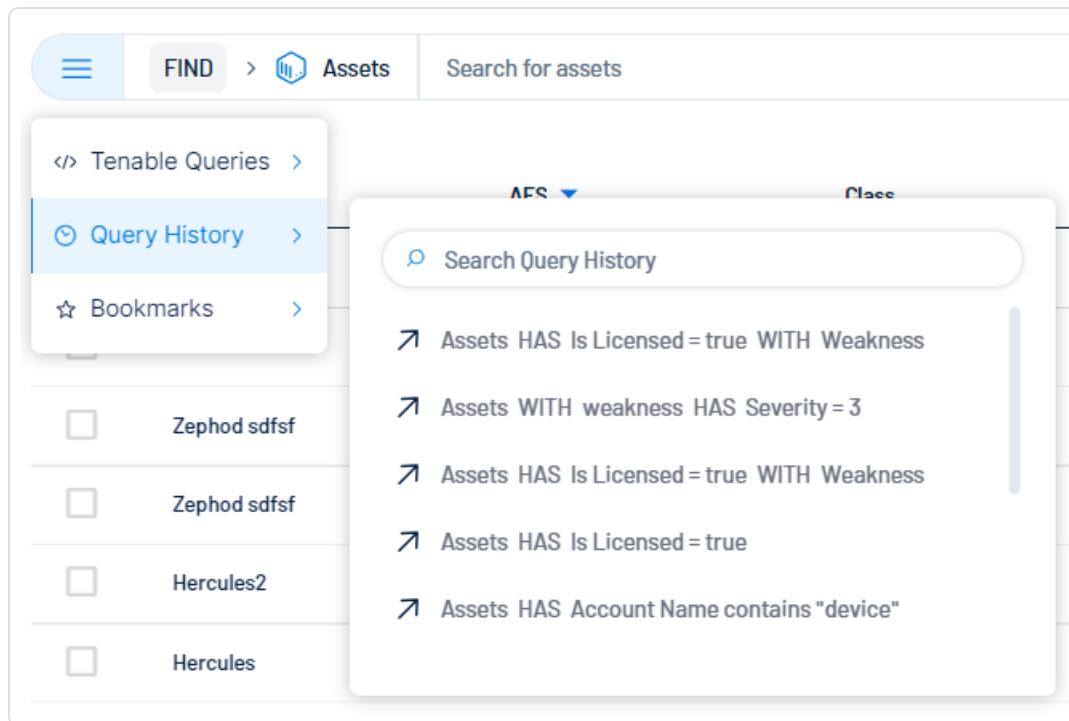
2. (Optional) Select a pre-defined query:

- **Tenable Queries** – Select from a list of Tenable-defined queries to search your assets.



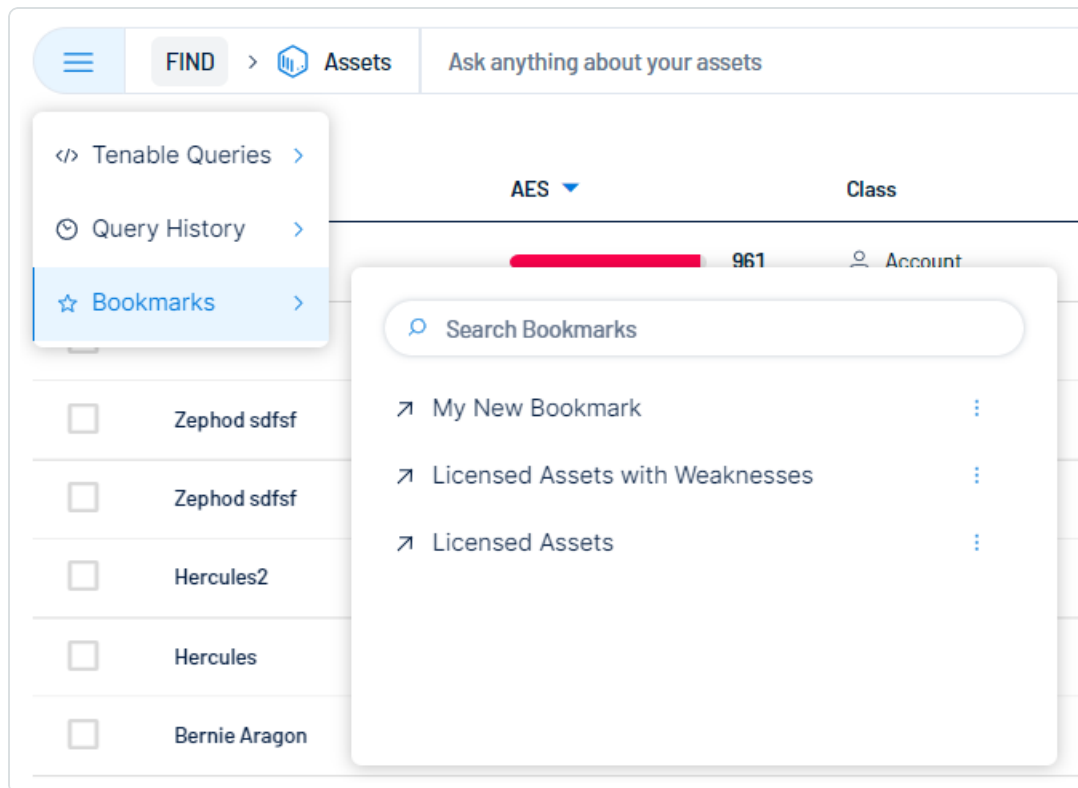


- **Query History** – Select from one of the most recently run queries to search your assets.





- **Bookmarks** – Select a pre-saved query bookmark to search your assets.



- To create a bookmark, [generate a query-based search](#) and [save the search as a bookmark](#).

- **To edit/delete a bookmark:**

- a. In the **Bookmarks** list, next to the bookmark you want to edit/delete, click the **⋮** button.

A menu appears.

- b. Do one of the following:

- To edit the bookmark, click **Edit**.

The **Edit Bookmark** window appears.



- i. Make any desired changes to the bookmark.
- ii. Click **Save**.

Tenable Exposure Management saves your changes to the bookmark.

**Tip:** Alternatively, you can edit the bookmark directly in the query text box. Make any desired changes to the query, then click **Save**.

- To delete the bookmark, click **Delete**.

A confirmation window appears.

- i. Click **Delete**.

Tenable Exposure Management deletes the bookmark from the **Bookmarks** list.

### 3. Select the type of search you want to run:

**Tip:** For additional information and examples on how to use the global asset search, see the [Global Asset Search Quick Reference Guide](#).

- **Start a search based on a query string:**

You can generate a search query to search for specific assets across Tenable Exposure Management.

**Example query strings:**

Try one or more of the following queries to get started:

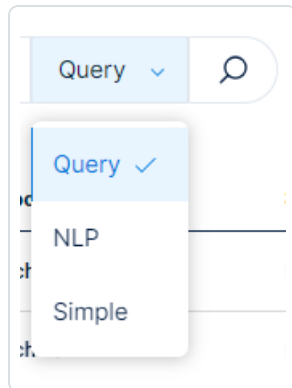
```
AS Device HAS (high_vuln_count > 5 AND acr > 8) OR (critical_vuln_count > 10)
```

```
AS Account HAS ( asset_name CONTAINS "admin" and aes > 700 ) WITH Weakness HAS severity > 2`
```



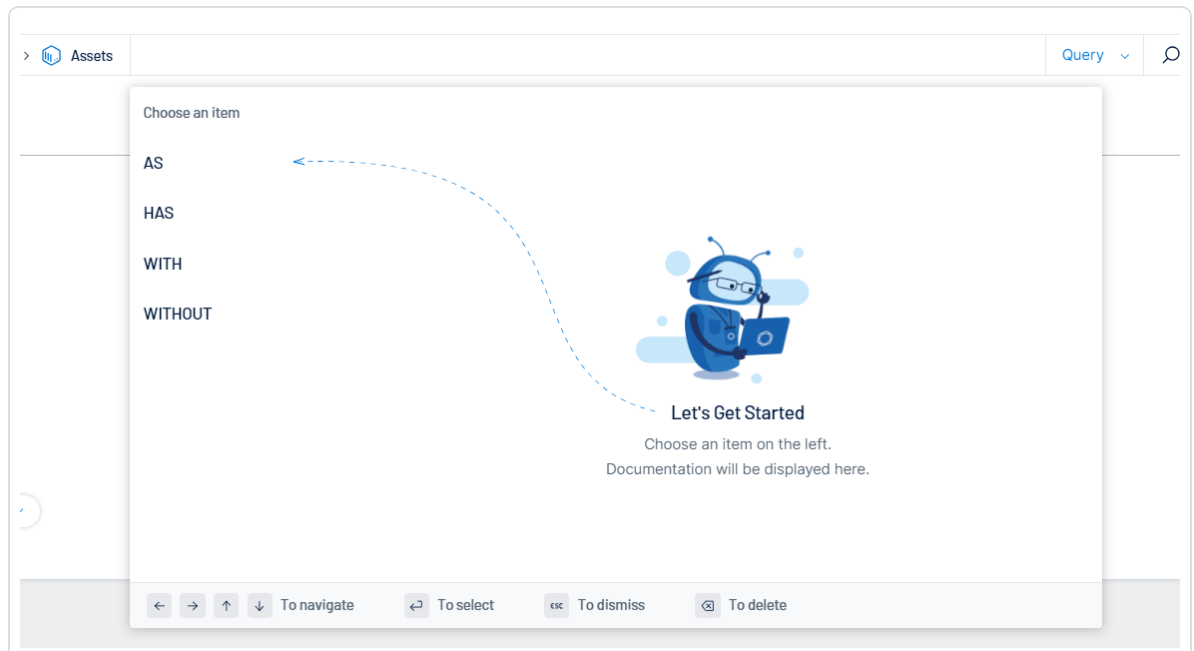
AS Account WITH Weakness HAS weakness\_name contains "Missing MFA"

- a. On the right side of the global search bar, in the drop-down, select **Query**.



- b. Click inside the **Search for Assets** text box.

The search query builder appears.



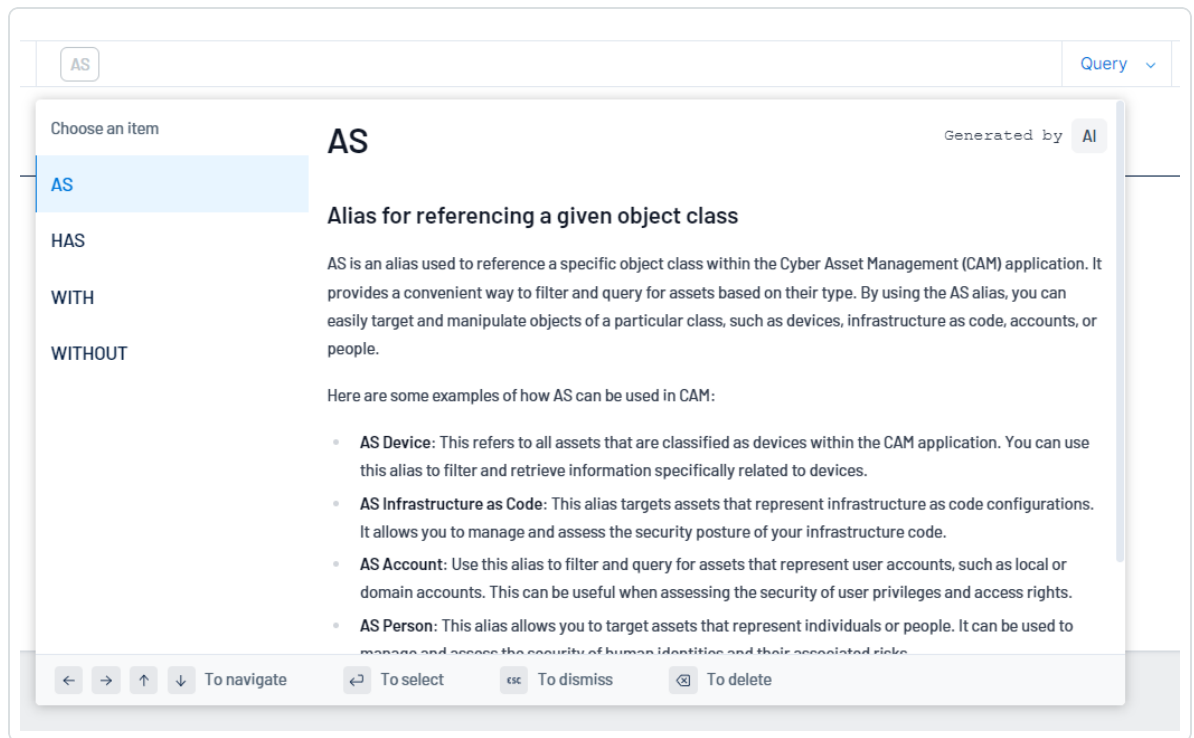
**Tip:** You can also build your query using your keyboard. Follow the instructions on the bottom of the query builder to navigate.

- c. On the left side of the query builder, choose an operator to begin your search.



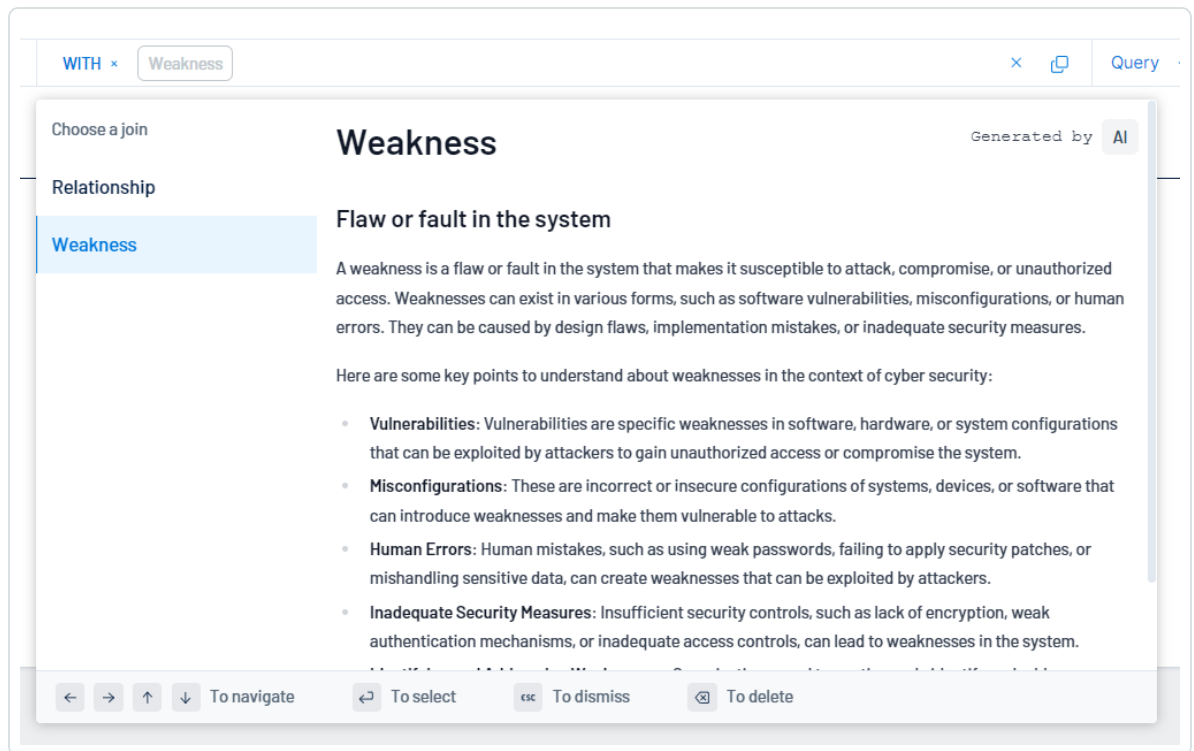


**(Not supported in [FedRAMP environments](#))** Hover your mouse cursor over an item to view an AI-generated description of how the operator filters your assets.



d. Select a qualifier for your query.

**(Not supported in [FedRAMP environments](#))** Hover your mouse cursor over an item to view an AI-generated description of how the item filters your assets.



**Note:** Tenable Exposure Management only displays qualifiers and operators that generate a working query. You cannot select items that break the query string.

- e. (Optional) Where applicable, add additional items and qualifiers to the query.

**Tip:** Click on a query token to edit that section of the query without starting over!

- f. On the right side of the search bar, click the  button.

Tenable Exposure Management performs the search and filters the asset list based on your query.

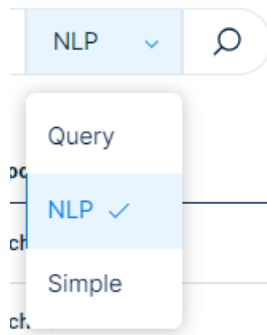
#### Start a search based on Natural Language Processing:

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

You can use Natural Language Processing (NLP) to ask questions about your assets and receive AI-generated answers.

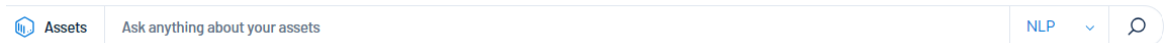


- a. On the right side of the global search bar, in the drop-down, select **NLP**.



- b. In the **Ask anything about your assets** text box, type a question you want to ask about your assets. For example, you could ask *"How many critical assets do I have?"*.

**Tip:** For more suggestions on questions to ask based on your business context, see [NLP Search Use Cases](#).



Tenable Exposure Management performs a search and provides an AI-generated response to your question. Additionally, the system parses the question and generates a token query based on the question. You can view and copy this query from the search bar.

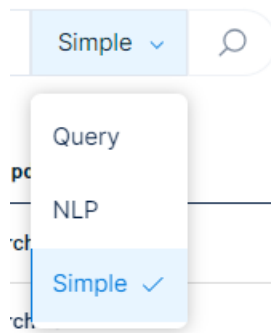
This response only includes information related to your asset query. If no data is available, an error message appears indicating no data could be generated for the search criteria you entered.


- **Perform a Simple search:**

A **Simple** search allows you to filter your asset list by asset name or asset ID.






- a. On the right side of the global search bar, in the drop-down, select **Simple**.



- b. In the **Search by asset name or asset ID** text box, type the asset name or asset ID by which you want to filter the asset list.
- c. On the right side of the search bar, click the  button.

Tenable Exposure Management performs the search and filters the asset list based on your query.


What to do next:

- To clear the search, in the search query text box, click the  button.
- To copy the search, in the search query text box, click the  button.
- To save the search as a bookmark, click the  button.

**A Bookmark Added window appears.**

- a. In the **Name** text box, type a name for the bookmark.
- b. (Optional) In the **Description** text box, type a description for the bookmark.
- c. Click **Save**.

A **Bookmark Added** confirmation message appears, and Tenable Exposure Management saves the bookmark to the [Bookmarks](#) list.

- To create a [Tag](#) based on the query results, click  **Create**.

**A menu appears.**



- a. Click **Tag**.

You navigate directly to the [Create New Tag](#) page.

- To create an [Exposure Signal](#) based on the query results, click **+ Create**.

#### A menu appears.

- a. Click **Exposure Signal**.

You navigate directly to the [New Exposure Signal](#) page.

## NLP Search Use Cases

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

When you use the [Natural Language processing](#) option in the [Global Asset Search](#), you can ask questions about your assets and receive AI-generated answers. The following are some examples of questions you might ask based on your business context. Additionally, you can view the expected [Query](#) search input for each example.

Context	Question	Expected Query
As a security practitioner, I want to ensure that all my devices are scanned.	Show me all my recently scanned Assets	Assets HAS last_updated > "2024-03-11"
As a security practitioner, I want to control my most critical assets.	Show me my assets with high criticality rating	Assets HAS external_criticality_score >= 8
As a security practitioner, I want to know who is using my devices.	Show me all accounts connected to a device	Assets AS Account WITH Relationship = Account -> Device
As a security practitioner, I want to locate all the laptops within my organization.	Show me all devices with "laptop" in their hostname	Assets AS Device HAS host_name contains "laptop"
As a security practitioner, I want to	Show me all devices	Assets AS Device WITH



find all of my computers impacted by CVE-2014-2014.	impacted by CVE-2014-2014	Weakness HAS weakness_name = "CVE-2014-2014"
As a security practitioner, I want to find all my devices that have a high vulnerability count and Asset Criticality Rating.	Show me my assets with high vulnerability count and ACR	Assets HAS Number of Total Weaknesses>10 AND ACR>5
As a security practitioner, I want to find all my accounts that have the name "admin".	Show me my accounts with the name "admin"	Assets AS Account Has Account name="admin"
As a security practitioner, I want to view my most critical assets.	Show me my assets with ACR above 8	Assets HAS ACR>8
As a security practitioner, I want to prioritize my assets that have a high Asset Exposure Score.	Show me my assets with a high AES	Assets HAS AES>=800
As a security practitioner, I want to find all my devices with a weakness where the name contains the text "Missing MFA".	Show me my accounts that have a weakness with "missing mfa" in the name	Assets AS Account WITH weakness HAS Weakness Name containers "missing mfa"

## Asset Details

On the [Assets](#) page, you can view additional details for any asset in the assets list.

**Note:** Information on the asset details page varies depending on the [class](#) of the asset for which you're viewing details. For example, an **Identity** asset features different tabs and data than a **Device** asset.

**Important:** Because they do not include a hardware ID attribute, Microsoft Entra ID devices managed by Microsoft Intune's mobile device management (MDM) are not visible on the Assets page.

To view asset details:

1. Access the [Assets](#) page.
2. In the row of the asset for which you want to view details, click **See details**.



The asset details page appears.

← Back to Inventory Summarize

DEVICE  
**jenkins-aws**  
Last Observed At: 20 Jul 2025 at 10:12 • 2 Sources: • [Show Details](#)

Asset Exposure Score  
 **981/1000**

Asset Criticality Rating  
 **3/10** Default

Findings Identified  
 **28** [See in Findings](#)

Key Properties  

Asset Class	Device
Asset Type	—
Asset Functionality	—
Last Observed At	20 Jul 2025 at 10:12

[Properties](#) [Connectors Details](#) [Score Breakdown](#) [Active Findings](#) [Weaknesses](#) [Tags](#) [Exposure Cards](#) [Software](#) [Exposure Signals](#) [Relationships](#) [Users](#) [Device Accounts](#)

Search...

**Key Properties**

Asset Class	Device	Created Date	1 Feb 2024 at 11:38
Last Observed At	20 Jul 2025 at 10:12		

**Asset Cluster Logic**

Asset Provider ID

On the asset details page, you can:

**Note:** Some of the following items only appear for specific asset classes.


- View the **Asset Name**.
- View the [asset class](#), for example, **Device**.
- View the number of and the icons for each [exposure category](#) associated with the asset.
- Click **Show Details** to view additional asset information:
  - **Info** — A brief description of the asset, when it was created, and when it was last seen.
  - **Tenable Data Sources** — The [data sources](#) associated with the asset. Click on a data source name to navigate directly to that application.
- **Generate and view an AI summary of the asset:**



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).



Tenable Exposure Management allows you to generate a summary of your asset using AI. Summaries are generated at the container level, and only apply to licensed assets within your container.

**Note:** Tenable Exposure Management limits the number of summaries you can generate to 100 per hour, with a maximum of 1000 summaries per day.

 **Delete**

 **Hide Summary** 





About this asset Gen AI

Unauthorized Access and Control

The TenableRole is an AWS role that grants users excessive privileges, potentially allowing unauthorized access and control over sensitive resources. This role has not been used for its intended purpose in over 90 days, indicating potential overprovisioning or lack of proper access management. The role's overly permissive permissions pose a significant risk to the organization, as it could be exploited by malicious actors to perform unauthorized actions, escalate privileges, or compromise sensitive data.

**Weaknesses**

The most critical risk associated with the TenableRole is its overprivileged nature. The role grants users broader permissions than necessary, increasing the attack surface and making it more vulnerable to compromise. This misconfiguration could allow unauthorized individuals to access sensitive information, modify or delete critical resources, or even escalate privileges to gain complete control over the AWS environment.

  |  

Do one of the following:





- To generate an AI summary for the asset for the first time, in the upper-right corner of the page, click **Summarize**.

Tenable Exposure Management uses AI to generate a summary of the asset including general details and specifics about the asset's weaknesses.

- To view an existing AI summary for the asset, in the upper-right corner of the page, click **Show Summary**.

Tenable Exposure Management displays the previously generated AI summary for the asset.

**Tip:** Click the button to copy the summary directly to your clipboard. You can also rate the helpfulness of the summary by clicking or to help improve the quality of AI-generated content within Tenable Exposure Management in the future. Click to regenerate the AI summary for the asset.

- View the **Asset Exposure Score** for the asset.

**Note:** Tenable Exposure Management does not calculate an AES for unlicensed assets. For more information, see [Tenable Exposure Management Metrics](#).

- View the **Asset Criticality Rating** for the asset.
- View the number of **Findings Identified** on the asset. Click **See in Findings** to navigate directly to the [Findings](#) page.
- View high-level **Key Properties**, including:
  - **Asset Class** — The [asset class](#) associated with the asset, for example, **Device**.
  - **Owner** — The owner of the asset.
  - **Drivers** — The key drivers of (that is, plugins that have the biggest effect on) the asset.
  - **Location** — The physical location of the asset.
  - **Last Observed At** — The date and time at which a scan most recently identified the asset.

When viewing the asset details page, you can click on the following tabs to view additional asset information:



**Tip:** Each tab includes a search box, where you can search for specific items.

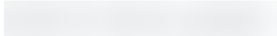

## Properties

The **Properties** section highlights details about the asset's properties.

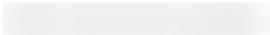

**Key Properties**

<b>Asset Class</b>	Resource	<b>Created Date</b>	15 Jul 2025 at 15:36
<b>Last Observed At</b>	22 Jul 2025 at 02:42		

**Asset Cluster Logic**

**Cloud Resource ID**  

**Asset Information (6)** [Show More](#)










<b>Asset ID</b>		<b>Asset Name</b>	annam-cloud-run-00001-79n
<b>Is Licensed</b>	Yes	<b>Last Update Date</b>	22 Jul 2025 at 02:42
<b>Pending Delete</b>	No	<b>Sources</b>	

Here, you can view asset details including:

**Note:** The properties listed in the user interface depend on the asset for which you are viewing details.

Key Properties	
Item	Description
Asset Class	The <a href="#">asset class</a> associated with the asset, for example, <b>Device</b> .
Created Date	The date and time at which the asset source first created the asset record.



Host Fully Qualified DNS	The Host Fully Qualified Domain Names, or FQDNs, of the asset host.												
Host System Type	The type associated with the asset's host system, for example, <b>general-purpose</b> .												
Last Observed At	The date and time at which a scan most recently identified the asset.												
Show information order	<div><p>Click to view the source order in which Tenable Exposure Management pulls asset property data for multi-source assets.</p><div><p><b>Property Merge Order: Asset Name</b> <span>×</span></p><p>Prioritized sequence of sources used when merging assets, determining which source's data becomes the unified asset's property. <a href="#">Learn more</a></p><div><div><div></div></div><div>Search by source name or value</div></div><table><tr><th>Order</th><th>Source</th><th>Source Value</th></tr><tr><td>1</td><td> HackerOne neww</td><td>https://vulcan.io/</td></tr><tr><td>2</td><td> Outpost24 NEww</td><td>vulcan.io</td></tr><tr><td>3</td><td> RiskRecon Neww</td><td>vulcan.io</td></tr></table></div></div>	Order	Source	Source Value	1	 HackerOne neww	https://vulcan.io/	2	 Outpost24 NEww	vulcan.io	3	 RiskRecon Neww	vulcan.io
Order	Source	Source Value											
1	 HackerOne neww	https://vulcan.io/											
2	 Outpost24 NEww	vulcan.io											
3	 RiskRecon Neww	vulcan.io											

## Asset Cluster Logic (Multi-source assets only)

### Description

An explanation of why a third-party asset was merged with one or more other sources. For each merged asset, you can view the matching criteria and value (e.g., hostname, IP address, MAC address etc.) that triggered the merge.

Merging criteria is based on a set of predefined asset properties relevant to the asset's class. Icons indicate the individual sources from which the asset data was clustered.

**Tip:** Hover over the icon to view details about the asset source.



#### Wiz Issues

Exposure Category

Vendor

Cloud Security

Wiz

### Asset Information

Item	Description
ACR	The Asset Criticality Rating associated with the asset. For more information, see <a href="#">Tenable Exposure Management Metrics</a> .
AES	The Asset Exposure Score associated with the asset. For more information, see <a href="#">Tenable Exposure Management Metrics</a> .
Application SSL Enabled	Indicates whether or not Application SSL is enabled on the asset.
Asset ID	The asset's UUID.
Asset Name	<p>The asset identifier; assigned based on the presence of certain attributes in the following logical order:</p> <ol style="list-style-type: none"><li>1. Nessus Agent name</li><li>2. Hostname</li><li>3. WebApp hostname</li><li>4. Container Security Image name</li><li>5. Container Runtime hostname</li><li>6. Cloud Common Resource name</li></ol>



	<ul style="list-style-type: none"><li>7. Cloud Common Resource identifier</li><li>8. Cloud Runtime name</li><li>9. Cloud IAC name</li><li>10. Active Directory Asset name</li><li>11. Domain Record hostname</li></ul> <p>If none of the above attributes are present, then <b>FQDN</b> is selected as the name for the asset.</p>
Cloud is Autoscale	Indicates whether or not the asset is part of a cluster that can automatically scale its size.
Cloud is lac	Indicates whether or not the asset is Infrastructure as Code (IaC).
Cloud is Real	Indicates whether or not the asset is actively running in the cloud.
Device Sub Classes	Where applicable, the subclass associated with the asset device.
Device System Type	Where applicable, the system type associated with the asset device.

## Connectors Details

Connectors are how Tenable Exposure Management syncs and integrates with tools and third-party data. The **Connectors Details** section shows details about all connectors associated with the asset.

**Tip:** For more information, see [Connectors](#).

Properties

Connectors Details

Score Breakdown

Attack Paths

Weaknesses

Tags

Exposure Cards

Software

Exposure Signals

...

Search Connector

Tenable Web Application Scanning

Show raw data

ServiceNow ITAM

Show raw data

SentinelOne Singularity

Show raw data

Click **Show raw data** to view the raw data for the connector.

## Accounts

The **Accounts** section shows a list of tiles with information about accounts associated with the asset.

Properties

Accounts

Devices

Tags

Attack Paths

Liveboard

Weaknesses

Entitlements

Roles

Groups

Access

More

aaron.aaron@alsid.corp

aaron.aaron@alsid.corp

aaron.aaron@alsid.corp

aaron.aaron@alsid.corp

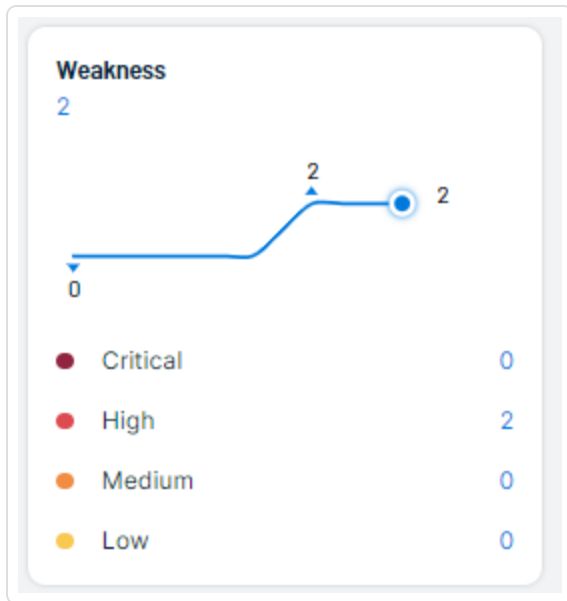
aaron.aaron@alsid.corp

**Tip:** At the bottom of the page, use the horizontal scroll bar to view all listed accounts.

Each tile includes the following information:



- **Key Properties:**
  - **Class** — The [asset class](#) associated with the asset, for example, **Account**.
  - **Category** — The category associated with the asset, for example, **ACCOUNT**.
  - **Description** — Where available, a description of the account.
- **Network and Administrator Profile:**
  - **OU** — The Organizational Unit (OU) associated with the account.
  - **Domain** — The domain associated with the account. For more information, see [Domains](#) in the *Tenable Identity Exposure User Guide*
  - **Forest Name** — The forest name associated with the account. For more information, see [Forests](#) in the *Tenable Identity Exposure User Guide*.
- **Account Provider** — The provider of the account, for example, **Azure Active Directory**.
- **Account AES** — The overall [Asset Exposure Score](#) associated with the account.
- **Last Use** — The date on which the account was most recently accessed by a user.
- **Last Location Used** — The physical location of where the account was most recently used.
- **Account Activity** — The activity status of the account, for example, **Active**.
- **Weakness** — A graphical representation of weaknesses on the account. This section includes a line graph and an individual count of each weakness and its criticality. For more information, see [Weaknesses](#).



## Devices

The **Devices** section shows all devices associated with the asset. This list highlights the hosts used by an account. Each device and its relevant information is listed as a tile on the page.





lucqa-afad-clie

### Key Properties

**Class**

**Category**  
general-purpose

**Description**  
-

**Drivers**  
NESSUS:11936, NESSUS:171410:DYNAMIC\_IP

### Network and administrator profile

**Static IP Assignment**  
10.200.200.6

**OU**  
-

**Domain**  
alsid.corp

**Forest Name**  
-

**Device AES**  
548

**Weakness**  
14

	Critical	1
	High	8
	Medium	5
	Low	0

**Last Use**  
10/04/2024, 07:13:20

**User**  
-

**Last Location Used**  
10.200.200.6

**Identities Associated With The Device**

**Devices Using MFA**

**Device OS** ACTIVE  
Microsoft Windows Server 2019 Datacenter 10.0.17763

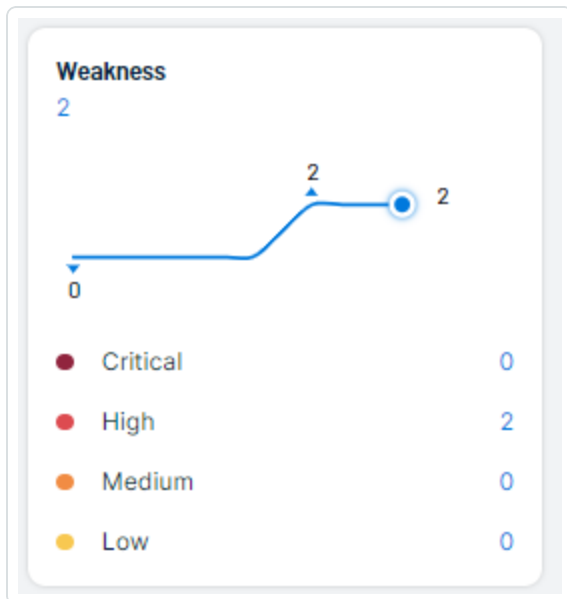
On each tile, you can view the following device information:

- **Key Properties:**

- **Class** – The [asset class](#) associated with the device.
- **Category** – The category associated with the device, for example, **general-purpose**.



- **Description** – Where available, a description of the device.
- **Drivers** – A list of drivers installed on the device.
- **Network and Administrator Profile:**
  - **Static IP Assignment** – The static IP address associated with the device.
  - **OU** – The Organizational Unit (OU) associated with the device.
  - **Domain** – The domain associated with the device. For more information, see [Domains](#) in the *Tenable Identity Exposure User Guide*
  - **Forest Name** – The forest name associated with the device. For more information, see [Forests](#) in the *Tenable Identity Exposure User Guide*.
- **Device AES** – The overall [Asset Exposure Score](#) associated with the device.
- **Weakness** – A graphical representation of weaknesses on the device. This section includes a line graph and an individual count of each weakness and its criticality. For more information, see [Weaknesses](#).



- **Last Use** – The date on which the device was most recently accessed by a user.
- **Last User** – The last user account to access the device.
- **Last Location Used** – The physical location of where the account was most recently used.



- **Identities associated with the Device** – Where applicable, any Active Directory or Microsoft Entra ID Identities associated with the device.
- **Devices Using MFA** – Indicates if the device requires multi-factor authentication (MFA) for user login.
- **Device OS** – The operating system (OS) running on the device. In the upper-right corner of the box, view a color-coded status of the OS, for example, **Active**.

## Attack Paths

The **Attack Paths** section shows a table list of the top attack paths in which the asset is present.

**Tip:** As part of a typical attack, adversaries leverage different tools and techniques to accomplish their objectives. This event is known as Attack Path. An attack path contains one or more Attack Techniques, allowing the hacker to accomplish their objective. To see a full list of supported attack paths within Tenable Exposure Management, view the [Tenable Attack Path Techniques](#) list.

Properties

Score Breakdown

Liveboard

Attack Paths

Weaknesses

Tags

Exposure Cards

Relationships

Search for an attack path or priority...

Search

Name	Path Priority Rating ^	Nodes	
undefined to undefined	● High	🔑 → 📁	<a href="#">See in APA</a>
undefined to undefined	● High	🔑 → 📁	<a href="#">See in APA</a>
undefined to undefined	● High	🔑 → 📁 → 📁	<a href="#">See in APA</a>
undefined to undefined	● High	🔑 → 📁 → 📁	<a href="#">See in APA</a>
undefined to undefined	● High	🔑 → 📁 → 📁	<a href="#">See in APA</a>

The attack paths list includes the following information:

- **Name** – The name of the attack path.
- **Path Priority Rating** – The priority of an attack path. Tenable Exposure Management calculates the PPR based on the relative number of attack paths to critical assets. Tenable Exposure Management categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**.
- **Nodes** – A visual representation of the nodes involved in the attack path that indicates the node type and the order in which the nodes might be accessed.








- **See in APA** – Click **See in APA** [↗](#) in the row of any attack path to navigate directly to the [Top Attack Paths](#) page with the selected attack path displayed by default.

## Active Findings

The **Active Findings** section shows a table list of all active findings associated with the asset.

**Important:** This section only contains data from ACTIVE (Active, New, and Resurfaced) findings. FIXED findings data is not included.

**Tip:** For more information, see [Findings](#).

Properties	Connectors Details	Score Breakdown	Active Findings	Weaknesses	Tags	...
<input type="text" value="Search..."/> <input type="button" value="Search"/>						
Finding Name <span>▼</span>	Severity	State	Last Seen	Solutions		
Vms exposed to the public with critical vulnerabilities	 Critical	Active	15 July 2025	-	<a href="#">See details</a>	>
VM/serverless infected with a high/critical severity malware	 Critical	Active	15 July 2025	-	<a href="#">See details</a>	>
VM/serverless infected with a hacking tool	 High	Active	15 July 2025	-	<a href="#">See details</a>	>
VM with Vul	 Medium	Active	15 July 2025	-	<a href="#">See details</a>	>
VM infected with malware is communicating with a malicio...	 Critical	Active	15 July 2025	-	<a href="#">See details</a>	>
Resource with vulnerabilities with high chance of being ex...	 High	Active	15 July 2025	-	<a href="#">See details</a>	>
Resource with cleartext cloud keys granting high privileges	 Medium	Active	15 July 2025	-	<a href="#">See details</a>	>

The weaknesses table includes the following information:

- **Finding Name** – The name of the finding.
- **Severity** – The severity of the finding, for example, **Critical**.
- **State** – The state of the active finding, for example **Active** or **Resurfaced**.
- **Last seen** – The date at which the weakness was last seen in a scan on the asset.
- **Solutions** – Where applicable, a brief description of how you can remediate the finding.



- Click **See details** to view more details about a finding. For more information, see [Finding Details](#).

## Weaknesses

The **Weaknesses** section shows a table list of all weaknesses associated with the asset.

**Tip:** For more information, see [Weaknesses](#).

<div>PropertiesScore BreakdownLiveboardAttack PathsWeaknessesTagsExposure CardsRelationships</div>							
<div>Q Search...Search</div>							
Weakness Name	Type	Description	Severity ^	VPR	Impacted Assets	Source	Last Seen
CVE-2022-30190	Vulnerability	<p>A remote code execution	Critical	9.8	20	NESSUS	28 December 2023
CVE-2022-24521	Vulnerability	Windows Common Log File :	Critical	9.4	15	NESSUS	28 December 2023
CVE-2022-22718	Vulnerability	Windows Print Spooler Elev:	Critical	9.7	15	NESSUS	28 December 2023
CVE-2022-21999	Vulnerability	Windows Print Spooler Elev:	Critical	9.7	15	NESSUS	28 December 2023
CVE-2022-26904	Vulnerability	Windows User Profile Servic	Critical	9.2	15	NESSUS	28 December 2023
CVE-2022-21916	Vulnerability	Windows Common Log File :	Critical	9	14	NESSUS	28 December 2023
CVE-2022-21919	Vulnerability	Windows User Profile Servic	Critical	9.5	14	NESSUS	28 December 2023

The weaknesses table includes the following information:

- **Weakness Name** – The Common Vulnerability Exposure (CVE) ID associated with the weakness.
- **Type** – The type of weaknesses: **Misconfiguration** or **Vulnerability**.
- **Description** – A brief description of the weakness.
- **Severity** – The severity of the weakness, for example, **Critical**.

**Note:** At this time, Tenable Exposure Management does not include information for Info level severity weaknesses.

- **VPR** – The [Vulnerability Priority Rating](#) (VPR) of the weakness.
- **Impacted Assets** – The number of assets impacted by the weakness. For more information, see [Assets](#).



- **Source** – The application the weakness' asset originated from, for example, Tenable Vulnerability Management.
- **Last seen** – The date at which the weakness was last seen in a scan on the asset.
- Click **See details** to view more details about a weakness. For more information, see [Weakness Details](#).

## Tags

The **Tags** section shows a table list of all tags applied to the asset.

**Tip:** For more information, see [Tags](#).

Properties   Score Breakdown   Liveboard   Attack Paths   Weaknesses <b>Tags</b> Exposure Cards   Relationships						
Search...						Search
Tag Name	CES ▾	Related Assets	Weaknesses	Source	Last Updated	
jo not exists	<div><div></div></div> 53	4,103	<div><div></div></div> 4911	Tenable.io	8 May 2023	<a href="#">See details</a> >
jo >5	<div><div></div></div> 55	4,164	<div><div></div></div> 4918	Tenable.io	8 May 2023	<a href="#">See details</a> >
jo net-q-p	<div><div></div></div> 55	4,164	<div><div></div></div> 4918	Tenable.io	8 May 2023	<a href="#">See details</a> >
jo noxists	<div><div></div></div> 55	4,164	<div><div></div></div> 4918	Tenable.io	8 May 2023	<a href="#">See details</a> >
One all	<div><div></div></div> 363	73	<div><div></div></div> 4284	Tenable One	20 March 2023	<a href="#">See details</a> >
jo Windows	<div><div></div></div> 650	26	<div><div></div></div> 4797	Tenable.io	6 December 2022	<a href="#">See details</a> >

- **Tag name** – The name of the tag value or tag category.
- **CES** – The [Cyber Exposure Score](#) for the tag value or tag category. The CES represents Cyber Exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for the assets to which the tag is applied. Higher CES values indicate higher risk.
- **Related Assets** – The number of assets to which the tag is applied.
- **Weaknesses** – The weaknesses associated with the asset. For more information, see [Weaknesses](#).
- **Source** – The application the tag originated from, for example, Tenable Vulnerability Management.



- **Last updated** – The date on which a user last updated the tag.
- Click **See details** to view more details about a tag. For more information, see [Tag Details](#).

## Entitlements

The **Entitlements** section shows entitlement information for assets who have roles, either:

- [Assigned in Microsoft Entra ID](#)
- Enabled by [Tenable cloud scanning](#) the Active Directory and [adding the appropriate domain](#).

Properties	Accounts	Devices	Tags	Attack Paths	Liveboard	Weaknesses	Entitlements	Roles	Groups	More
<input type="text" value="Search..."/> <input type="button" value="Search"/>										
Entitlements	Trustees	Accessible resources	Roles	Account	Last Use					
microsoft.office365.webPortal/allEntities/standard/read	22	0	66	Abdul Abbott	February 25, 2024					
microsoft.office365.supportTickets/allEntities/allTasks	22	0	46	Abdul Abbott	February 25, 2024					
microsoft.office365.serviceHealth/allEntities/allTasks	22	0	42	Abdul Abbott	February 25, 2024					
microsoft.azure.serviceHealth/allEntities/allTasks	22	0	37	Abdul Abbott	February 25, 2024					

The entitlements section includes the following information:

- **Entitlements** – The name of the asset entitlement.
- **Trustees** – The number of trustees associated with the asset entitlement. Click the number to navigate directly to the page filtered by all assets to which these trustees have entitlements.
- **Accessible Resources** – The number of accessible resources associated with the asset entitlement. Click the number to navigate directly to the [Access](#) tab for the asset.
- **Roles** – The number of accessible resources associated with the asset entitlement. Click the number to navigate directly to the [Roles](#) tab for the asset.
- **Account** – The name and type of the account asset associated with the entitlement. Click the name to navigate directly to view details for that specific asset.
- **Last Use** – The date on which the entitlement was last used by the asset.

## Roles



The **Roles** section shows all roles assigned to the asset. For example, if this identity has roles assigned in Microsoft Entra ID, their details appear here.

**Tip:** For more information, see [Assign Microsoft Entra roles to Users](#).

Properties	Accounts	Devices	Tags	Attack Paths	Liveboard	Weaknesses	Entitlements	Roles	Groups	Access	More
<input type="text" value="Search..."/>											Search
Roles	Origin	Severity ^	Trustees	Entitlements	Last Use						
Azure AD Joined Device Local Administrator		Medium	9	2	30 November 2023						
User		Medium	951	126	30 November 2023						
Global Administrator		Critical	18	195	11 January 2024						

The roles list includes the following information:

- **Roles** – The name of the role assigned to the asset.
- **Origin** – An icon that indicates the origin provider of the account (for example, Azure AD).
- **Severity** – The overall severity of the asset, for example, **Critical**.
- **Trustees** – The number of trustees associated with the asset role.
- **Entitlements** – The number of entitlements to which the role has access.
- **Last Use** – The date on which the role was most recently used on the asset.

## Groups

The **Groups** section shows a list of groups to which the asset belongs. For example, if this asset is a member of groups in Microsoft Entra ID or Azure Active Directory, they appear here.

**Tip:** For more information, see:

- [Assign Identities to Groups in Microsoft Entra](#)
- [Active Directory Security Groups](#)



Properties

Accounts

Devices

Tags

Attack Paths

Liveboard

Weaknesses

Entitlements

Roles

Groups

Access

Score Breakdown

More

Q Search...

Search

Group	Account	AES ^	Members	Origin	
All users	Aaron Aaron	<div></div>	2008	<div></div>	<a href="#">See details</a>
All users	Aaron Aaron	<div></div>	2008	<div></div>	<a href="#">See details</a>

The groups list includes the following information:

- **Group** – The name of the group to which the asset belongs.
- **Account** – The name of the account on the asset that belongs to the group.
- **AES** – The overall [Asset Exposure Score](#) associated with the account.
- **Members** – The total number of assets that belong to the group.
- **Origin** – An icon that indicates the origin provider of the group (for example, Azure AD).
- Click **See details** to navigate directly to the asset details page for the selected group.

## Access

The **Access** section shows access information for assets who have roles, either:

- [Assigned in Microsoft Entra ID](#)
- Enabled by [Tenable cloud scanning](#) the Active Directory and [adding the appropriate domain](#).

Properties

Accounts

Devices

Tags

Attack Paths

Liveboard

Weaknesses

Entitlements

Roles









Groups

Access

More

Q Search...

Search

Asset Name	AES	Asset Class	Entitlements	Entitlement Origin	Trustees
Mihaela Lapčević	<div><div></div><div></div></div>	906  ACCOUNT	microsoft.directory/users/authentication...		11
Mihaela Lapčević	<div><div></div><div></div></div>	906  ACCOUNT	microsoft.directory/users/allProperties/a...		9
Mihaela Lapčević	<div><div></div><div></div></div>	906  ACCOUNT	microsoft.directory/users/basicProfile/u...		503
Mihaela Lapčević	<div><div></div><div></div></div>	906  ACCOUNT	microsoft.directory/roleAssignments/allP...		11

The access list includes the following information:

- **Asset Name** – The asset identifier of the asset.
- **AES** – The overall [Asset Exposure Score](#) of the asset.

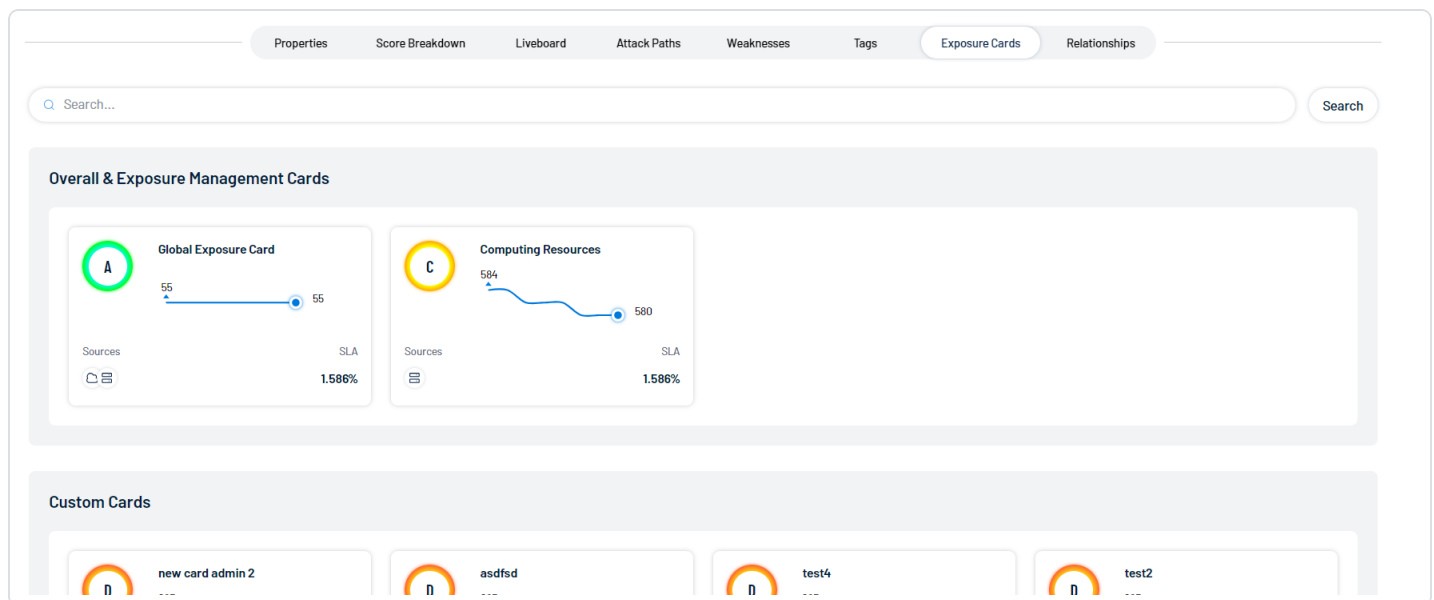


- **Asset Class** – The [asset class](#) associated with the asset, for example, **Account**.
- **Entitlements** – The directory path to which the asset has entitlement access.
- **Entitlement Origin** – An icon that indicates the origin provider of the entitlement (for example, Azure AD).
- **Trustees** – The number of trustees associated with the asset.

## Exposure Cards

The **Exposure Cards** section shows all exposure cards associated with the asset. Assets can be part of global exposure cards, or custom cards created by users on the [Exposure View](#) page.

**Tip:** An exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your Cyber Exposure Score (CES) and other metrics. Users can create custom cards, or use Tenable-provided cards to gain insight and guidance on what areas need their attention most.



Click on any card to navigate directly to the [Exposure View](#) page with the selected card data displayed by default.

For more information on exposure cards and how to create them, see the following:

- [Exposure Card Library](#)
- [Manage Exposure Cards](#)



## Relationships

The **Relationships** section shows a list of all assets with a known relationship to the current asset for which you are viewing details.

PropertiesAccountsDevicesTagsAttack PathsLiveboardWeaknessesEntitlementsRolesGroupsAccessScore BreakdownExposure CardsRelationships

Q Search...

Search

Relationship Type	Direction	Asset Name	Asset Class	AES ▾	Weaknesses	Last Updated	See details
Link a Person to all their Accounts	Source	Aaron Aaron	Account	<div><div></div></div> 778	<div><div></div></div> 2	5 January 2024	<a href="#">See details</a>
Link a Person to all their Accounts	Target	Aaron Aaron	Account	<div><div></div></div> 778	<div><div></div></div> 2	5 January 2024	<a href="#">See details</a>
Link a Person to all their Accounts	Source	Aaron Aaron	Account	<div><div></div></div> 772	<div><div></div></div> 1	4 January 2024	<a href="#">See details</a>
Link a Person to all their Accounts	Target	Aaron Aaron	Account	<div><div></div></div> 772	<div><div></div></div> 1	4 January 2024	<a href="#">See details</a>
Link a Person to all their Accounts	Source	Aaron Aaron	Account	-	<div><div></div></div> 0		<a href="#">See details</a>

The relationships list includes the following information:

- **Relationship Type** – The type of relationship between the two assets.
- **Direction** – Indicates whether the related asset is the **Source** or the **Target** of the asset relationship.
- **Asset Name** – The asset identifier of the related asset.
- **Asset Class** – The [asset class](#) associated with the asset, for example, **Account**.
- **AES** – The overall [Asset Exposure Score](#) of the related asset.
- **Weaknesses** – The weaknesses associated with the asset. For more information, see [Weaknesses](#).
- **Last Updated** – The date at which a scan most recently identified the asset.
- Click **See details** to navigate directly to the asset details page for the selected asset relationship.

## Software

The **Software** section shows, where available, the installed software on the asset.

**Note:** The **Software** section is only available for **Device** assets. For more information, see [Asset Classes](#).



Properties Score Breakdown Liveboard Attack Paths Weaknesses Tags Exposure Cards Relationships Software										
Search...										Search
Application Name ^	Publisher	Provider	Type	Versions	Associated Devices	Common Platform Enumeration	Bound Ports	File Locations	Last Seen Version	Last Seen
Libgcrypt	GnuPG		APPLICATION	1	5	2.3 * GnuPG, Libgcrypt, 1.8.5, * ...	0	1	1.8.5	Wed Feb 07 202...
OpenSSL	OpenSSL		APPLICATION	1	2	2.3 * OpenSSL, OpenSSL, 1.1.1f, ...	0	1	1.1.1f	Wed Feb 07 202...
Plex_Media_Server	ANY		APPLICATION	1	1	2.3 * * Plex_Media_Server, 1.3...	0	1	1.32.4.7195	Wed Feb 07 202...

The software list includes the following information:



- **Application Name** – The name of the software application installed on the asset.
- **Publisher** – The group or company that published the software application.
- **Provider** – The provider, or Tenable application, that discovered the software application.
- **Type** – The software type, for example, **Application**.
- **Versions** – The number of versions of the software installed on the asset.

Click a number to open the **Installed Versions** panel:



## OpenSSL Installed Versions



Last Seen Version ▾	Associated Devices	Last Seen
 3.0.8	2	Wed Feb 07 2024 19:35:40 GMT...
 1.0.2k	4	Wed Feb 07 2024 19:35:40 GMT...

Items per page

10 ▾

&lt; Previous page

1

Next page &gt;

1-2 of 2

In the **Installed Versions** panel, you can view the following information:

**Tip:** Use the **Search** box to search for a specific version of the installed software.

- **Last Seen Version** – The version of the software that was most recently seen on an asset.
- **Associated Devices** – The number of assets that have this version of the software installed.
- **Last Seen** – The date and time at which the software was most recently seen on an asset.
- **Associated Devices** – The number of assets that have this software application installed.
- **Common Platform Enumeration** – The Common Platform Enumeration (CPE) associated with the software application.



Click a CPE to open the **CPE** panel, where you can view information such as the **CPE Version**, **Vendor**, and **Product** for each version of the installed software.

## SQLite CPE ×

CPE Version	2.3
Part	*
Vendor	SQLite
Product	SQLite
Version	3.7.17
Software Update	*
Software Language	*
Target Software	*
Target Hardware	*

- **Bound Ports** — The number of ports on the asset that are bound to the software application.

**Note:** The **Bound Ports** option is only available for remotely detected devices.

Click a number to open the **Bound Ports** panel, where you can view the ports bound to the application as well as their associated devices:



## Libgcrypt Bound Ports



Port ▾

Associated Devices

8000

TCP

Items per page

10 ▾

< Previous page

1

Next page >

1-1 of 1

**Tip:** Use the **Search** box to search for a specific port or associated device.

- **File Locations** — The locations on your machine where the software application stores files.

Click a number to open the **File Locations** panel, where you can view the file paths for all locations where the software stores files.



# OpenSSL File Locations



Location ^

/opt/openssl/bin/openssl

/usr/lib64/libcrypto.so.1.0.2k

Items per page 10 ▼

< Previous page

1

Next page >

1-2 of 2

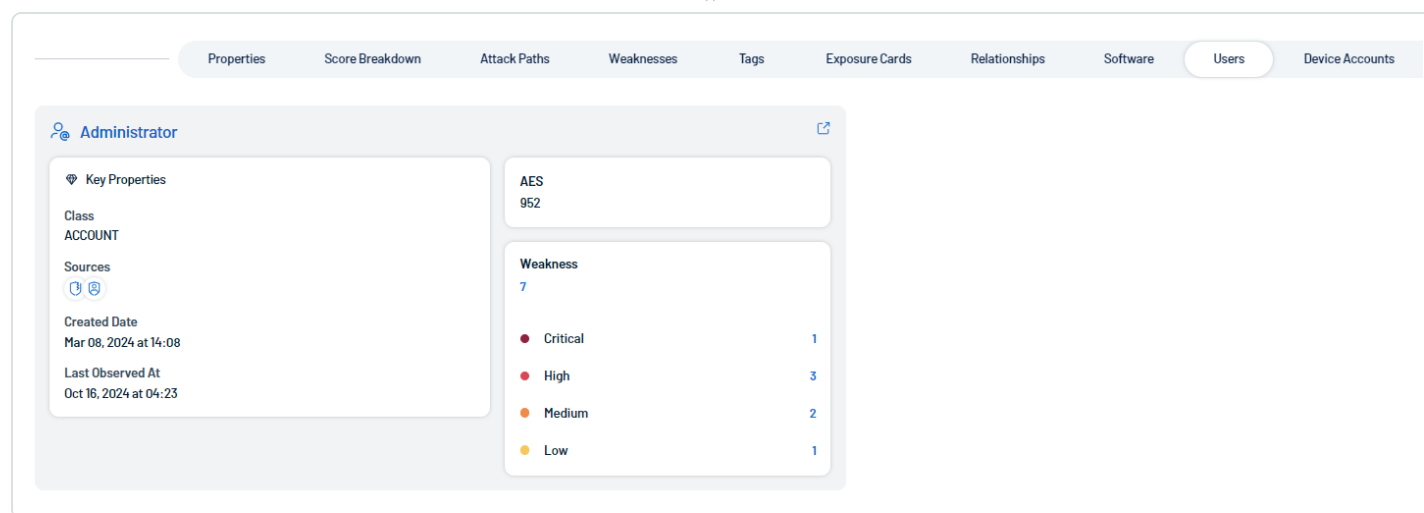
**Tip:** Use the **Search** box to search for a specific location.

- **Last Seen Version** – The version of the software that was most recently seen installed on an asset.
- **Last Seen** – The date and time at which the software was most recently seen on an asset.

## Users

The **Users** section shows a list of users with access to the device. Each user and its relevant information is listed as a tile on the page.

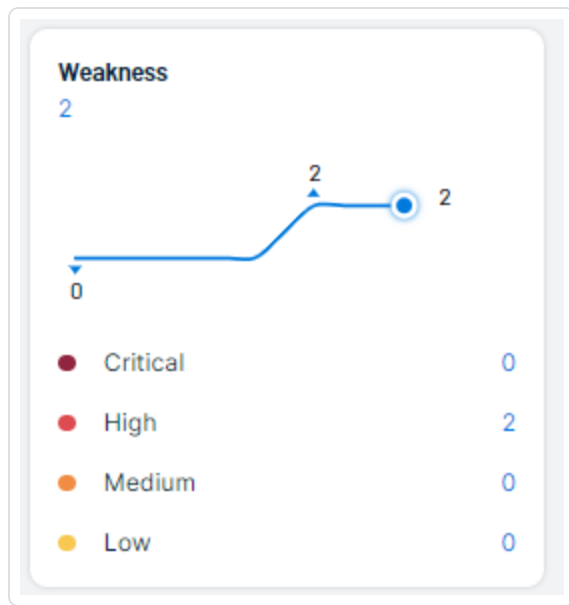




On each tile, you can view the following information about each user:

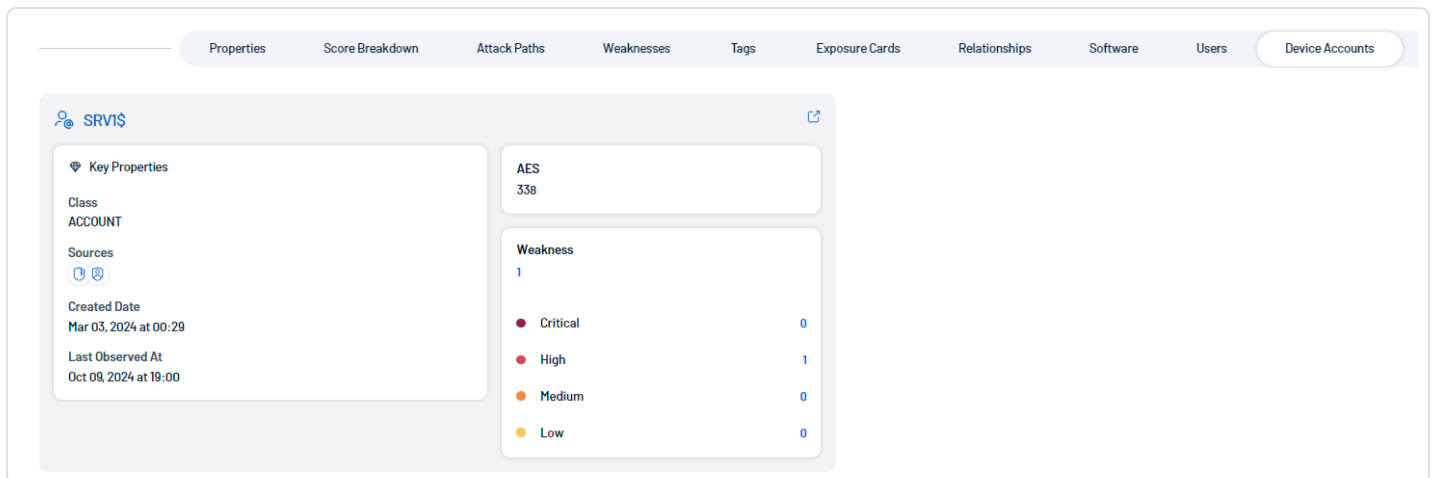
- **Key Properties:**
  - **Class** — The [asset class](#) associated with the user.
  - **Sources** — The application(s) the user originated from, for example, Tenable Vulnerability Management.
  - **Created Date** — The date and time at which the user was created.
  - **Last Observed At** — The date and time at which the user last accessed the device.
- **AES** — The overall [Asset Exposure Score](#) associated with the asset.
- **Weakness** — A graphical representation of weaknesses on the asset. This section includes a line graph and an individual count of each weakness and its criticality. For more information,

see [Weaknesses](#).



## Device Accounts

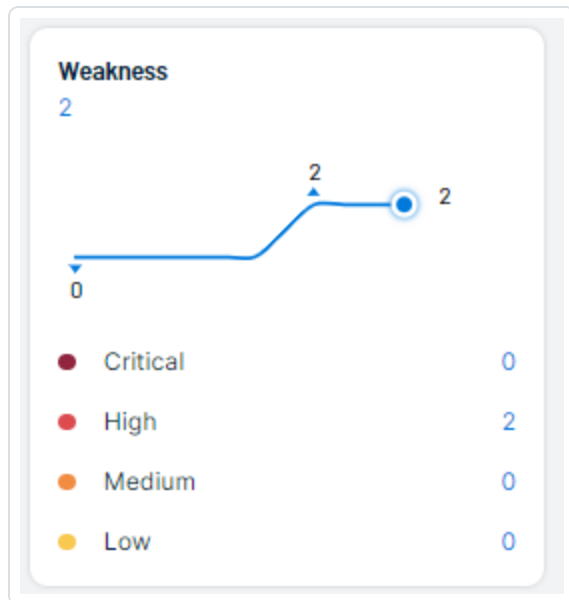
The **Device Accounts** section shows a list of all accounts present on a host. Each account and its relevant information is listed as a tile on the page.



On each tile, you can view the following information about each account on the account:

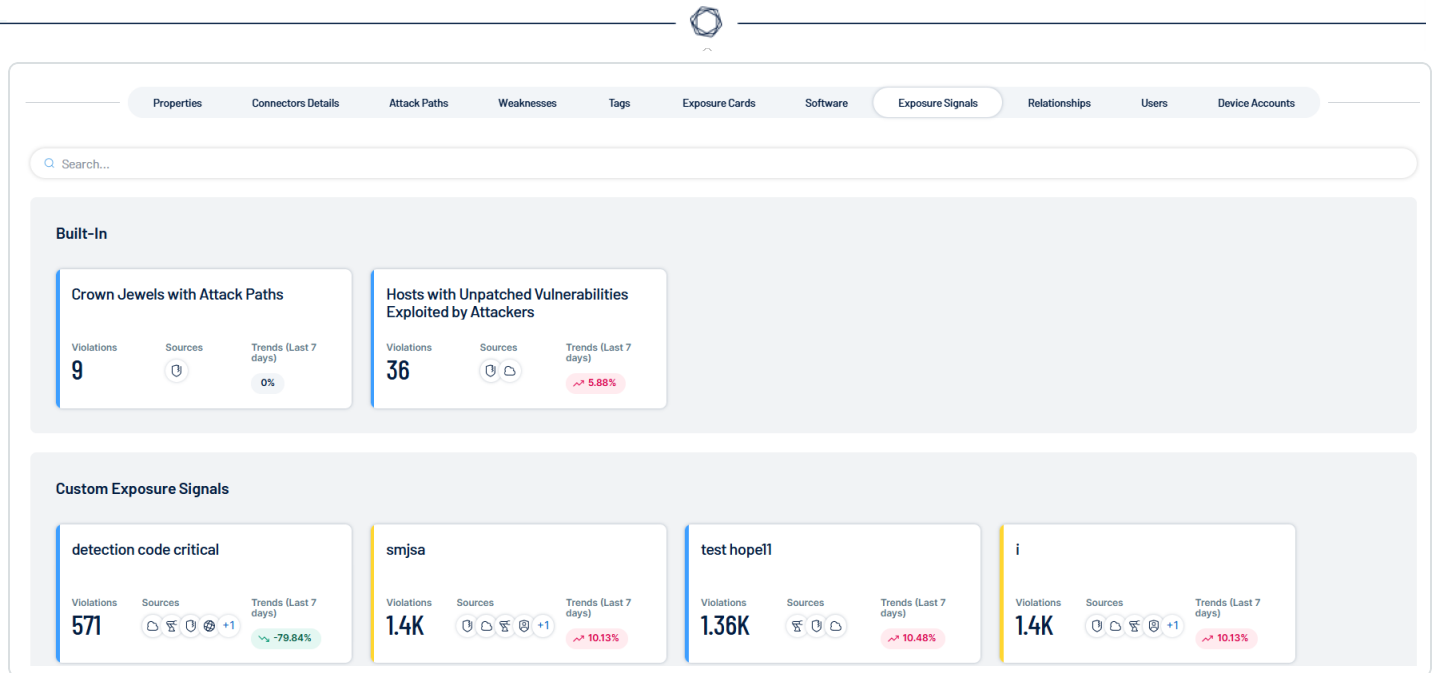


- **Key Properties:**
  - **Class** — The [asset class](#) associated with the account.
  - **Sources** — The application(s) the account originated from, for example, Tenable Vulnerability Management.
  - **Created Date** — The date and time at which the account was created.
  - **Last Observed At** — The date and time at which the a user last accessed the account.
- **AES** — The overall [Asset Exposure Score](#) associated with the asset.
- **Weakness** — A graphical representation of weaknesses on the asset. This section includes a line graph and an individual count of each weakness and its criticality. For more information, see [Weaknesses](#).




## Exposure Signals

The **Exposure Signals** section shows a list of tiles with information about [exposure signals](#) associated with the asset. An *Exposure Signal* can be defined as a combination of risks that could make any weakness potentially dangerous to your business.



Each tile includes the following information:

- **Severity** – Each card is color coded to indicate the severity associated with the exposure signals, for example:
  - Dark Red – Critical
  - Light Red – High
  - Orange – Medium
  - Yellow – Low
  - Blue – Info
- **Violations** – The number of assets found in violation of the exposure signal.
- **Exposure Mgmt.** – The [exposure category](#) associated with the exposure signal.
- **Trends** – The trend and percentage of change in violations within the last 7 days. For example, if the violations for this combination have increased by 5.45%, you'd see  5.45%.

Click on a tile to navigate directly to the [Exposure Signals](#) page filtered by the selected exposure signal.

## Tag Assets via the Assets Page

In the [Assets](#) view, you can apply tags directly to an asset in the asset list.

2 items selected ✕

Tag assets #

Merge assets ○

Adjust

#Computers:TAG-155-Create ✕

Add tag +

Assign tags Cancel

Name ▲

▼ ☒ asset1

Search te

Search results for 'te'

#Computers:TAG-155-Create

#Computers:Test Tag Scan

To apply an existing tag to an asset:

1. Access the [Assets](#) page.
2. In the asset list, select the check box next to any assets to which you want to apply the tag.
3. At the top of the asset list, click **Tag assets #**.

The **Add tag +** button appears.

4. Click **Add tag +**.

A **Search** box appears.

5. In the **Search** box, type the name of the tag you want to apply to the asset or assets.

**Tip:** To create a new tag, type the [category]:[value] pair and, at the bottom of the window, click **+**.

6. Click the name of the tag you want to apply to the asset or assets.

The tag appears above the asset list.

7. Repeat these steps for each additional tag you want to apply.
8. Click **Assign Tags**.

Tenable Exposure Management assigns the designated tags to the asset or assets.



To create a new tag:

1. Access the [Assets](#) view.
2. In the upper-right corner of the page, click **+ New Tag**.

The **Create a Tag** page appears.

[< Back to Tags](#)[Create Tag +](#)

## Create A Tag

Tag Category

Type Tag Category

Tag Value

Type Tag Value

Tag Type

StaticDynamic

Tag Description

Enter Tag Description

^ Include Assets (Optional)

Search for asset name or asset ID

<input type="checkbox"/>	Name	Sources	Class	AES	Weaknesses	Top Attack Techniques	Top Attack Paths	Associated Ta...	Last Updated
<input type="checkbox"/>	sql1		Device	892	3.7k	2	1	8	24 December 2024
<input type="checkbox"/>	srv1		Device	882	1.9k	8	1	6	25 December 2024
<input type="checkbox"/>	tenable-ad-sql		Device	872	899	1	0	6	12 December 2024
<input type="checkbox"/>	adfs1		Device	841	325	1	0	6	12 December 2024

3. Follow the steps for [creating a new tag](#).

## Weaknesses

Weaknesses are vulnerabilities and misconfigurations on your assets. The **Weaknesses** tab on the **Inventory** page highlights weaknesses on your assets and provides useful insights into those weaknesses, including descriptions, assets affected, criticality, and more.

**Note:** Only Active and Resurfaced vulnerabilities count towards your weaknesses.

To access the **Weaknesses** tab:



1. Do one of the following:

- In the left navigation menu, click **Inventory > Weaknesses**.
- At the top of the [Inventory](#) page, click the **Weaknesses** tab.

The **Weaknesses** tab appears.

The screenshot shows the 'Weaknesses' tab interface. At the top, there are three summary metrics: 'Number Of Weaknesses' (25.3k), 'New In Last 7 Days' (17.4k), and 'Number With VPR>7' (2k). Below these is a search bar and a filter dropdown set to 'All Weaknesses Types'. On the left, a 'Filters' sidebar is visible with categories like 'Sources', 'Tenable Sources', '3rd Party Connectors', and 'Weakness Type'. The main table lists various weaknesses with columns for Weakness Name, Description, Weakness Type, Severity, VPR (Beta), Impacted Assets, Top Attack Techniques, Last Seen, and See Details. The table includes entries for misconfigurations and vulnerabilities, with VPR values highlighted in red for critical items.

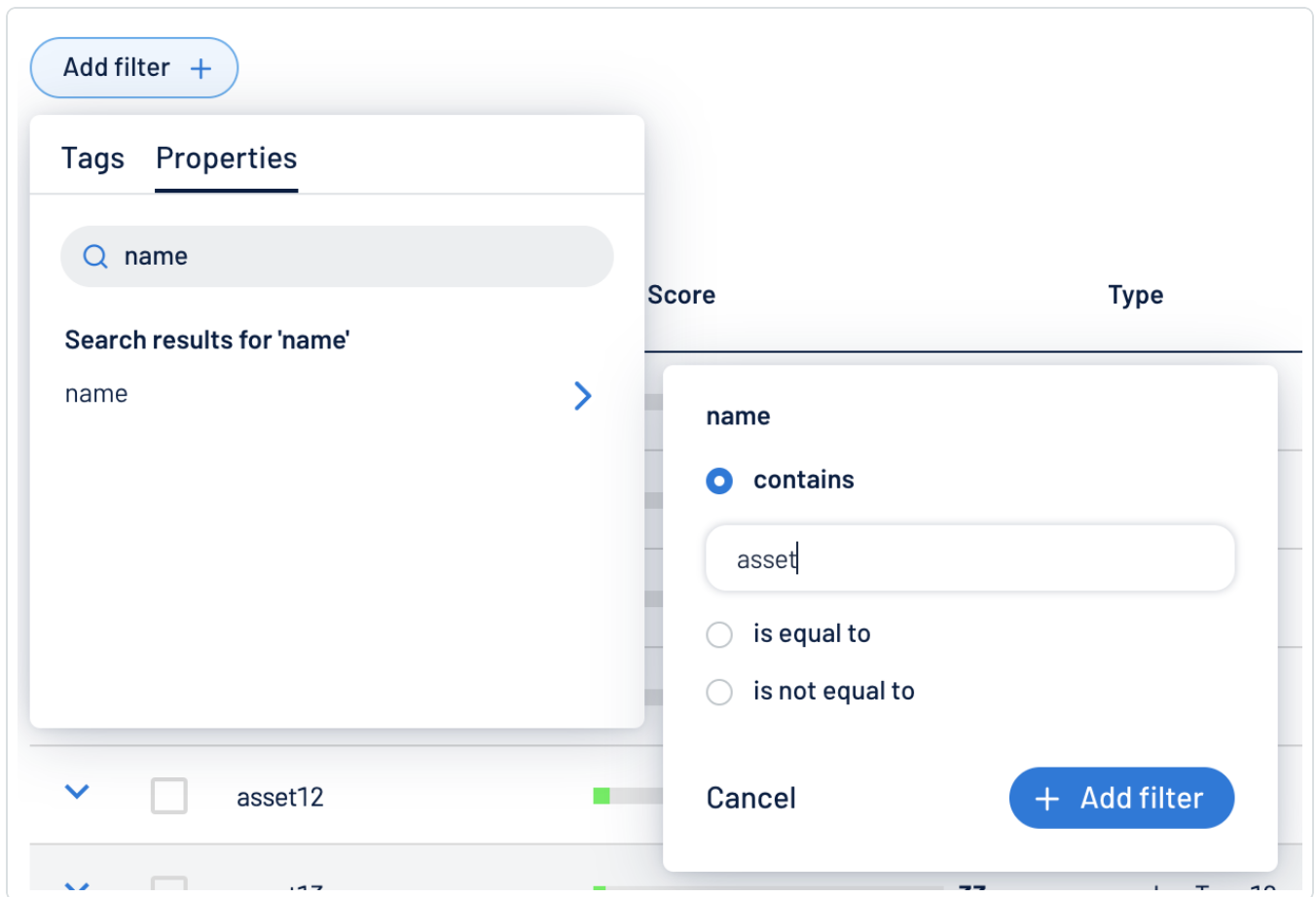
Weakness Name	Description	Weakness Type	Severity	VPR (Beta)	Impacted Assets	Top Attack Techniques	Last Seen	See Details
Too many members in a privileged ...	Too many administrators are present in the ...	Misconfiguration	Critical	-	1	0	9 May 2025	See Details >
Too many privileged accounts	Too many administrators are present in the ...	Misconfiguration	Critical	-	1	0	9 May 2025	See Details >
Overprivileged IAM User	Monitor IAM user privileges that were unus...	Misconfiguration	Critical	-	1	0	23 July 2025	See Details >
Virtual Machine has an unpatched ...	Virtual machines with vulnerabilities expose...	Misconfiguration	Critical	-	1	0	23 July 2025	See Details >
Virtual Machine has vulnerabilities ...	Virtual machines with vulnerabilities expose...	Misconfiguration	Critical	-	1	0	23 July 2025	See Details >
Kaspersky Endpoint Security Data...	Kaspersky Endpoint Security, a commercial ...	Misconfiguration	Critical	-	1	0	8 May 2025	See Details >
Oracle RDBMS Patchset Out of Date...	The version of Oracle Database server install...	Misconfiguration	Critical	-	1	0	8 May 2025	See Details >
Microsoft Windows 8 Unsupported...	The remote host is running Microsoft Wind...	Misconfiguration	Critical	-	1	0	8 May 2025	See Details >
CVE-2009-3933	Array index error in the SP5bvd protocol impl...	Vulnerability	Critical	-	1	0	8 May 2025	See Details >
CVE-2012-5335	Unspecified vulnerability in Adobe Flash Pla...	Vulnerability	Critical	9.6	1	0	8 May 2025	See Details >
CVE-2013-0633	Buffer overflow in Adobe Flash Player before...	Vulnerability	Critical	9.5	1	0	8 May 2025	See Details >
CVE-2013-0634	Adobe Flash Player before 10.3.185.51 and fl...	Vulnerability	Critical	9.5	1	0	8 May 2025	See Details >
CVE-2016-0051	The WebDAV client in Microsoft Windows Vi...	Vulnerability	Critical	9.4	1	0	8 May 2025	See Details >
CVE-2016-0728	The join_session_keyring function in securit...	Vulnerability	Critical	9.0	1	0	8 May 2025	See Details >

In the **Weaknesses** tab, you can:

- View the total number of weaknesses on assets within your container.
- View the total number of new weaknesses discovered within the last 7 days.
- View the total number of new weaknesses with a [Vulnerability Priority Rating](#) (VPR) greater than 7.
- In the weakness type drop-down, filter the list by the following weakness types:
  - **All Weakness Types**
  - **Misconfigurations**
  - **Vulnerabilities**

The weakness numbers at the top of the page and the weakness list update accordingly.

- Use the **Search** box to search for a specific weakness in the list.
- Filter the weaknesses list:



a. Click the  button.

The **Add filter**  button appears.

b. Click **Add filter** .

A menu appears.

c. Do one of the following:

- To search the weakness list by tag, click **Tags**.
- To search the weakness list by property, click **Properties**.

d. In the search box, type the criteria by which you want to search the list.

Tenable Exposure Management populates a list of options based on your criteria.





- e. Click the tag or property by which you want to filter the weakness list.

A menu appears.

- f. Select how to apply the filter. For example, if you want to search for a weakness whose name is *CVE-0000-0000*, then select the **contains** radio button and in the text box, type *CVE-0000-0000*.

- g. Click **Add filter** .

The filter appears above the asset list.

- h. Repeat these steps for each additional filter you want to apply.

- i. Click **Apply filters**.

Tenable Exposure Management filters the list by the designated criteria.

- Export the table or the page:

- a. (Optional) To export only specific table rows, in the table, select the check box next to the rows you want to export.

- b. Click the  button.

The **Export** window appears.



## Export



### General

☐ Entire Table ☐ Current Page ☒ Selected Rows (3)

### File Name

Enter a name for the exported file.

### Formats

☒ CSV

☐ JSON

### Columns

Search columns

☒ 9 of 9 fields selected

[View selected](#)

☒ AES

☒ Asset Class

☒ Asset Name

☒ Associated Tags Count

☒ Last Update Date

Cancel

Export



c. Do one of the following:

- To export the entire table, select the **Entire Table** radio button.

**Note:** When you export the entire table, Tenable Exposure Management only includes the first 50 columns. To view asset data for a larger number of assets, use the [Search Assets API](#) call.

- To export the current page, select the **Current Page** radio button.
- To export the selected rows, select the **Selected Rows** radio button.

d. In the **File Name** text box, type a file name to give the exported file.

e. In the **Formats** section, select the format in which you want to export the data.

f. In the **Columns** section, select the check box for each column you want to include in the export file.

g. Click **Export**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.


- Customize the columns in the table:

a. Click **Columns** .

The **Customize columns** window appears.

b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.

c. (Optional) In the **Show/Hide** section, select/deselect the checkboxes to show or hide columns in the table.

d. (Optional) In the **Remove** section, click the  button to permanently remove a column from the table.

e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.



- i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

- ii. Select the checkbox next to any column or columns you want to add to the table.

- iii. Click **Add**.

The column appears in the **Customize columns** window.

- f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

- g. Click  **Apply Columns**.

Tenable Exposure Management saves your changes to the columns in the table.

- View a list of your weaknesses, including the following information:
  - **Weakness Name** — The Common Vulnerability Exposure (CVE) ID associated with the weakness.
  - **Description** — A brief description of the weakness.
  - **Weakness Type** — The type of weaknesses: **Misconfiguration** or **Vulnerability**.
  - **Severity** — The severity of the weakness, for example, **Critical**.

**Note:** At this time, Tenable Exposure Management does not include information for Info level severity weaknesses.

**Note:** Because Tenable Exposure Management calculates CVEs using VPR and Tenable Cloud Security calculates using CVSS, you may notice a difference in severity across weaknesses between these applications.

- **VPR (Beta)** — The vulnerability's [vulnerability priority rating](#) using VPR (Beta) scoring.

**Tip:** For more information, see the [Scoring Explained](#) Quick Reference Guide.

- **Impacted Assets** — The number of assets impacted by the weakness. For more information, see [Assets](#).
- **Top Attack Techniques** — Instances of MITRE Att&ck techniques associated with this asset that are used in attack paths leading to critical assets. For more information, see



## [Top Attack Techniques.](#)

**Tip:** Click a choke point to navigate directly to the **Attack Techniques** tab on the [Attack Path](#) page, filtered automatically by techniques that feature the weakness.

**Note:** Because Tenable Exposure Management aggregates techniques by cause (for example, CVE, CWE) a single choke point may have multiple sources/targets. This may cause discrepancies in technique counts between the **Weaknesses** tab and the sum of choke points within the **Top Attack Techniques** tab.

- **Last seen** – The date at which the weakness was last seen in a scan on the asset.
- **Sources** – The application the weakness' asset originated from, for example, Tenable Vulnerability Management.
- Click **See details** to view more details about a weakness. For more information, see [Weakness Details](#).

## Weakness Details

In the **Weaknesses** view, you can view details for any weakness in the list.

To view weakness details:

1. Access the [Weaknesses](#) view.
2. In the row of the weakness for which you want to view details, click **See details**.



The weakness details page appears.

Weakness Name

configEnabled

Misconfiguration

Severity Level

High

VPR

Impacted Assets

27

See Assets

Top Attack Techniques

0

Last Seen

6 June 2024

First Seen

6 June 2024

Last Updated

8 September 2023

^ Description

Description:

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. The recorded information includes the configuration item (AWS resource), relationships between configuration items (AWS resources), any configuration changes between resources. It is recommended AWS Config be enabled in all regions.

Rationale:

The AWS configuration item history captured by AWS Config enables security analysis, resource change tracking, and compliance auditing.

It is recommended AWS Config be enabled in all regions.

^ Properties

Search

Show all properties

10/27 properties shown

Weakness Id

CS.AC\_AWS\_0632

Product Code

CS

Detection Code

AC\_AWS\_0632

Weakness Type

Misconfiguration

Detection Family

Logging and Monitoring

Provider Code

CS

Provider Detection ID

AC\_AWS\_0632

Detection Variant

PLUGIN

Detection Sub Category

MISCONFIGURED\_CLOUD\_SETTINGS

Detection Type

AWS

^ Impacted Assets

Search...

Name	Class	AES	Weaknesses	Top Attack Techniques	Top Attack Paths	Associated Tags Count	Last Updated	See Details
eu-west-1	Other Resource	0	4	0	0	4	14 August 2024	See Details >
eu-central-1	Other Resource	0	4	0	0	4	14 August 2024	See Details >

On the weakness details page, you can:

- View the **Weakness Name**.
- View the **Severity Level** of the weakness, for example, **Critical**.

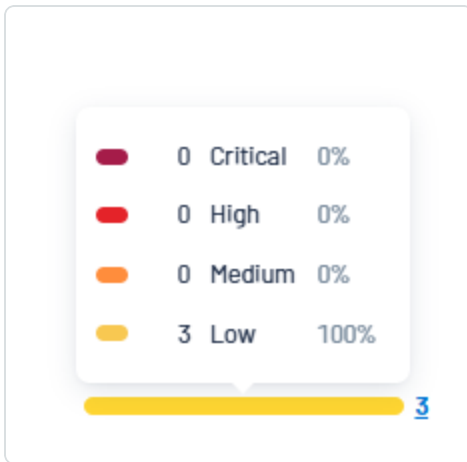
**Note:** Because Tenable Exposure Management calculates CVEs using VPR and Tenable Cloud Security calculates using CVSS, you may notice a difference in severity across weaknesses between these applications.

- View the [Vulnerability Priority Rating](#) (VPR) of the weakness.
- View the number of **Impacted Assets** associated with the weakness.
  - Click **See Assets** to scroll down to the full list of impacted assets.
- View the **Top Attack Techniques** for the weakness.

**Note:** Because Tenable Exposure Management aggregates techniques by cause (for example, CVE, CWE) a single choke point may have multiple sources/targets. This may cause discrepancies in technique counts between the **Weaknesses** view and the sum of choke points within the **Top Attack Techniques** view.



- Hover over the priority to view the full breakdown of the techniques associated with the weakness, and their relative criticalities.



- Click the metric to navigate directly to the [Top Attack Techniques](#) view, filtered automatically by attack path techniques that feature the weakness.
- View the date at which the weakness was **Last Seen** in a scan on the asset.
- View the date at which the weakness was **First Seen** in a scan on the asset.
- View the date at which the weakness was **Last Modified**.
- View the weakness' **Publication Date**.
- View a **Description** of the weakness.
- View a list of **Properties** associated with the weakness.

These can include, but are not limited to:

**Note:** The properties displayed in this section depend on the type of weakness for which you are viewing details.

- **Weakness ID** — The Common Vulnerability Exposure (CVE) ID associated with the weakness.
- **Weakness Type** — The type of weakness: **Misconfiguration** or **Vulnerability**.



- **Detection Family** – The detection family associated with detecting the weakness, for example, **CVEs**.
- View a table list of the **Impacted Assets** associated with the weakness.

This list includes the following information:

- **Name** – The asset identifier. Tenable Exposure Management assigns this identifier based on the presence of certain asset attributes in the following order:
  1. Agent Name (if agent-scanned)
  2. NetBIOS Name
  3. FQDN
  4. IPv6 address
  5. IPv4 address

For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.

- **AES** – The [Asset Exposure Score](#) for the asset. The AES represents the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

**Note:** Tenable Exposure Management does not calculate an AES for unlicensed assets.

- **Class** – The class type associated with the asset. For more information, see [Asset Classes](#).
- **Weaknesses** – The weaknesses associated with the asset. For more information, see [Weaknesses](#).

**Tip:** Click on a Weakness count to navigate directly to the **Weaknesses** view.

- **Top Attack Techniques** – Instances of MITRE Att&ck techniques associated with this asset that are used in attack paths leading to critical assets. For more information, see [Top Attack Techniques](#).





**Tip:** Click a choke point to navigate directly to the **Top Attack Techniques** view on the [Attack Path](#) page, filtered automatically by techniques that feature the weakness.

**Note:** Because Tenable Exposure Management aggregates techniques by cause (for example, CVE, CWE) a single choke point may have multiple sources/targets. This may cause discrepancies in technique counts between the **Weaknesses** view and the sum of choke points within the **Top Attack Techniques** view.

- **Top Attack Paths** – Instances of attack paths associated with this asset that lead to critical assets. For more information, see [Top Attack Paths](#).

**Tip:** Click a choke point to navigate directly to the **Top Attack Paths** view on the [Attack Path](#) page, filtered automatically by attack paths that feature the weakness.

- **Associated Tags** – The number of tags applied to the asset. For more information on tagging an asset, see [Tag Assets via the Assets Page](#).
- **Last updated** – The date and time at which the asset was last updated.
- Click **See details** to view more details about an asset. For more information, see .

## Findings

A finding is a single instance of a weakness (vulnerability or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol. The **Findings** tab on the **Inventory** page highlights findings on your assets and provides useful insights into those findings, including descriptions, assets affected, criticality, and more. By providing comprehensive information about your findings, Tenable Exposure Management helps to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.

To access the **Findings** tab:

1. Do one of the following:
  - In the left navigation menu, click **Inventory** > **Findings**.
  - At the top of the [Inventory](#) page, click the **Findings** tab.

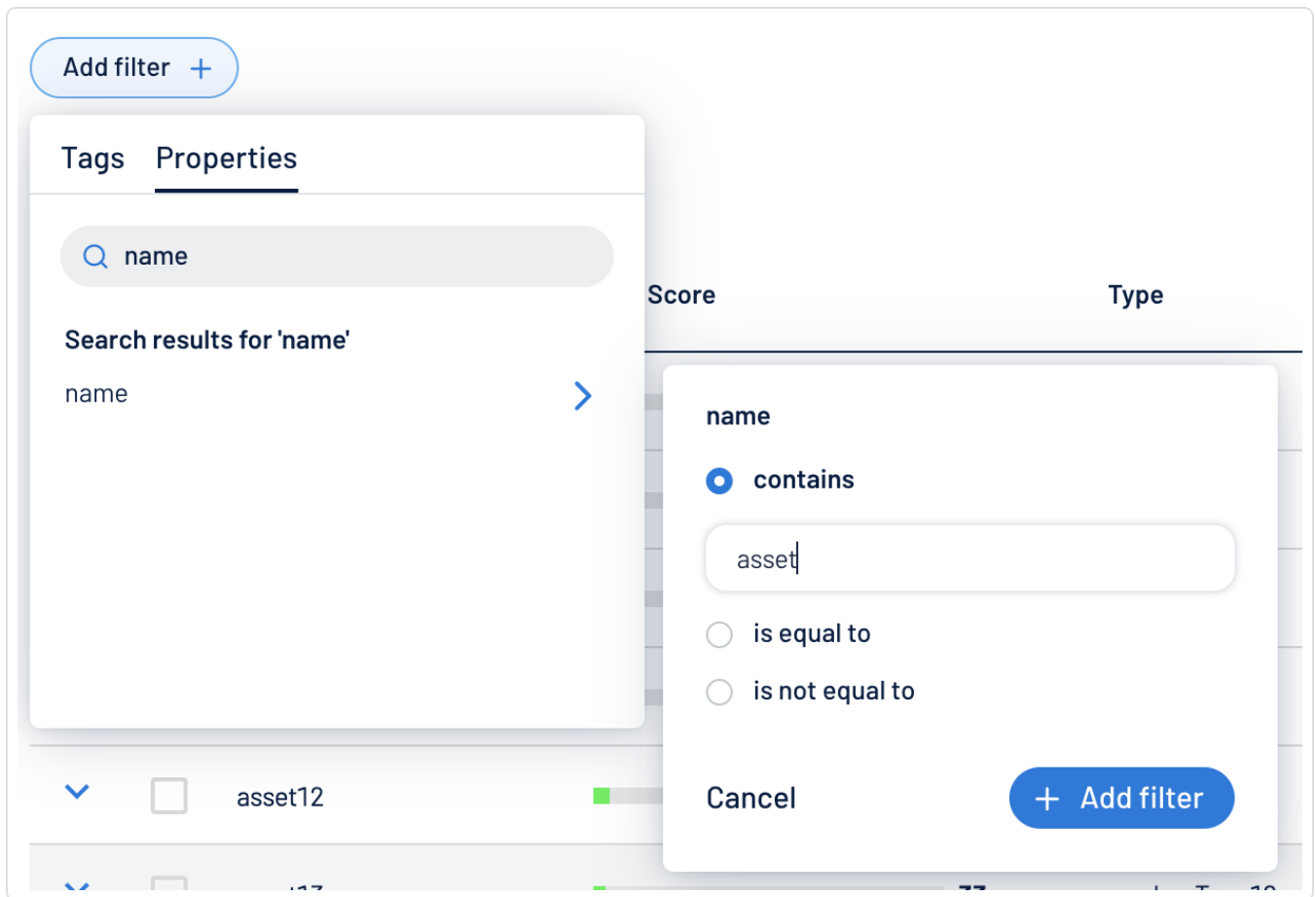
The **Findings** tab appears.

The screenshot displays the 'Findings' tab interface. At the top, there are three summary metrics: 'Total Findings' (304.8k), 'Critical & High Findings' (42.8k), and 'New (in the last 7 days)' (121.7k). Below these is a search bar labeled 'Search by Finding Name or Finding ID'. To the left of the main table is a 'Filters' sidebar with sections for 'Sources' (Attack Surface M..., Cloud Security, Container Security, Identity Exposure, OT Security, Security Center, Vulnerability Man..., Web Application ...), '3rd Party Connectors' (Crowdstrike, Microsoft TVM, Outpost24), and 'Findings Type'. The main table shows a list of findings with columns: Finding Name, Asset Name, Severity, State, Solution, VPR (Beta), and See Details. The table is currently showing 304,795 findings, grouped by severity. The first few findings are all 'Critical' and 'ACTIVE', with VPR values ranging from 8.9 to 9.7. Each finding has a checkbox on the left and a 'See Details' link on the right.

	Finding Name	Asset Name	Severity	State	Solution	VPR (Beta)	See Details
<input type="checkbox"/>	Security Update for Microsoft Offi...	dir-win10-eng	Critical	ACTIVE	Microsoft has released a set of pat...	9.7	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	Security Updates for Microsoft Offi...	dir-win10-eng	Critical	ACTIVE	Microsoft has released KB5002620 ...	8.9	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	KB5018616: Windows 10 Version 20...	dir-win10-info	Critical	ACTIVE	Apply Security Update 5018616	9.2	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	KB5013952: Windows 10 Version 18...	dcl	Critical	ACTIVE	Apply Security Update 5013952	7.9	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	CVE-2019-2899	dir-win10-info	Critical	ACTIVE	—	-	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	Security Update for Microsoft Offi...	dir-win10-eng	Critical	ACTIVE	Microsoft has released a set of pat...	9.7	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	KB5048652: Windows 10 version 21...	dir-win10-eng	Critical	ACTIVE	Apply Security Update 5048652	9.5	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	MS16-148: Security Update for Micr...	dir-win10-eng	Critical	ACTIVE	Microsoft has released a set of pat...	9.7	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	KB5077308: Windows 10 Version 20...	dir-win10-info	Critical	ACTIVE	Apply Security Update 5077308	9.4	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	CVE-2024-24691	dir-win10-eng	Critical	ACTIVE	—	-	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	CVE-2024-23917	dir-win10-eng	Critical	ACTIVE	—	-	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	KB5022834: Windows 10 Version 2...	dir-win10-info	Critical	ACTIVE	Apply Security Update 5022834	9.2	<a href="#">See Details &gt;</a>

In the **Findings** tab, you can:

- View the total number of findings on assets within your container.
- View the total number of new findings discovered within the last 7 days.
- View the total number of new findings with a [Vulnerability Priority Rating](#) (VPR) greater than 7.
- Use the **Search** box to search for a specific finding in the list.
- Filter the findings list:



a. Click the  button.

The **Add filter**  button appears.

b. Click **Add filter** .

A menu appears.

c. Do one of the following:

- To search the findings list by tag, click **Tags**.
- To search the findings list by property, click **Properties**.


d. In the search box, type the criteria by which you want to search the list.

Tenable Exposure Management populates a list of options based on your criteria.



- e. Click the tag or property by which you want to filter the findings list.

A menu appears.

- f. Select how to apply the filter. For example, if you want to search for finding related to Windows, then select the **contains** radio button and in the text box, type *Windows*.
- g. Click **Add filter** .

The filter appears above the asset list.

- h. Repeat these steps for each additional filter you want to apply.
- i. Click **Apply filters**.

Tenable Exposure Management filters the list by the designated criteria.

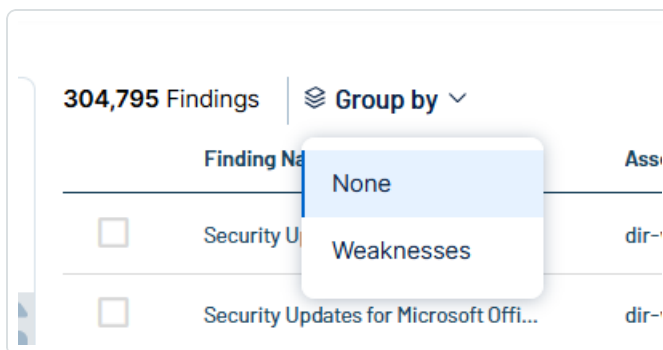
- Group your findings by weakness:

To reduce noise within your findings list, you can group your findings by their associated weakness.

**Tip:** For more information, see [Weaknesses](#).

- a. Above the list, click **Group by** .

A menu appears.



- b. Click **Weaknesses**.

Tenable Exposure Management groups your findings by their associated weakness. Click



the [>](#) button for any weakness group to view the full list of findings within that group.

26,486 Weaknesses

Group by: Weaknesses

Weakness Name		Description	Weakness Type	Severity	VPR (Beta)	See Details
<div><div></div></div>	Tenable Virtual Appliance Unsuppo...	The remote host is a Tenable Virtual Applian...	Misconfiguration	<div><div></div>Critical</div>	<div>-</div>	<a href="#">See Details</a>

1 Active Finding

Finding Name	Asset Name	Severity	State	Solution	Last Seen	See Details
Tenable Virtual A...	tenapp48.target....	<div><div></div>Critical</div>	ACTIVE	Replace Tenable Virtual A...	6 August 2025	<a href="#">See Details</a>

- Export the table or the page:
  - a. (Optional) To export only specific table rows, in the table, select the check box next to the rows you want to export.
  - b. Click the [↗](#) button.

The **Export** window appears.



## Export



### General

☐ Entire Table ☐ Current Page ☒ Selected Rows (3)

### File Name

Enter a name for the exported file.

### Formats

☒ CSV

☐ JSON

### Columns

Search columns

☒ 9 of 9 fields selected

[View selected](#)

☒ AES

☒ Asset Class

☒ Asset Name

☒ Associated Tags Count

☒ Last Update Date

Cancel

Export



c. Do one of the following:

- To export the entire table, select the **Entire Table** radio button.

**Note:** When you export the entire table, Tenable Exposure Management only includes the first 50 columns. To view asset data for a larger number of assets, use the [Search Assets API](#) call.

- To export the current page, select the **Current Page** radio button.
- To export the selected rows, select the **Selected Rows** radio button.

d. In the **File Name** text box, type a file name to give the exported file.

e. In the **Formats** section, select the format in which you want to export the data.

f. In the **Columns** section, select the check box for each column you want to include in the export file.

g. Click **Export**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.


- Customize the columns in the table:

a. Click **Columns** .

The **Customize columns** window appears.

b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.

c. (Optional) In the **Show/Hide** section, select/deselect the checkboxes to show or hide columns in the table.

d. (Optional) In the **Remove** section, click the  button to permanently remove a column from the table.

e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.



- i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

- ii. Select the checkbox next to any column or columns you want to add to the table.

- iii. Click **Add**.

The column appears in the **Customize columns** window.

- f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

- g. Click  **Apply Columns**.

Tenable Exposure Management saves your changes to the columns in the table.

- View a list of your findings, including the following information:
  - **Finding Name** — The name of the finding.
  - **Asset Name** — The name of the asset on which the finding exists.
  - **Severity Level** — The severity of the finding, for example, **Critical**.

**Note:** At this time, Tenable Exposure Management does not include information for Info level severity findings.

- **State** — The state of the finding, for example **ACTIVE** or **FIXED**.
- **Solution** — A brief description of how you can remediate the finding.
- **VPR Score (Beta)** — The vulnerability's [vulnerability priority rating](#) using VPR (Beta) scoring.

**Tip:** For more information, see the [Scoring Explained](#) Quick Reference Guide.

- **Sources** — The application the finding's asset originated from, for example, Tenable Vulnerability Management.
- Click **See details** to view more details about a finding. For more information, see [Finding Details](#).

## Finding Details

In the **Findings** view, you can view details for any finding in the list.





To view finding details:

1. Access the [Findings](#) view.
2. In the row of the finding for which you want to view details, click **See details**.

The finding details page appears.

[< Back to findings](#)

VULNERABILITY

## Flash Player <= 11.7.700.260 / 12.0.0.43 Unspecified Remote Code Execution (APSB14-04)

**CRITICAL** **ACTIVE** | Last Observed: 29 September 2024 at 10:49 | 1 Source

Finding ID: 0001e338-3498-4b94-9946-2211e3b44af4

VPR

**9.5/10**

Top Attack Techniques

**2**

[See in APA](#)

Detection Timeline

Last Seen: 29 September 2024  
First Seen: 19 June 2022  
Last Updated: 29 September 2024

**Solution**

Upgrade to Adobe Flash Player version 11.7.700.261 / 12.0.0.44 or later.

### Properties

[Show all properties](#) 10/64 properties shown

Finding ID	0001e338-3498-4b94-9946-2211e3b44af4	State	ACTIVE
Detection ID	NESSUS:72284	Last Updated	29 September 2024 at 10:49
First Seen	19 June 2022 at 09:30	Last Seen	29 September 2024 at 10:49
Original Risk Severity Level	4	Cpes	cpe:/a:adobe:flash_player
Active Finding Count	786	Fixed Finding Count	1063

### Weaknesses

Name	Type	Severity	VPR	Description	Impacted Assets	Sources
------	------	----------	-----	-------------	-----------------	---------

On the finding details page, you can:

- View the name of the finding.
- View the severity of the finding, for example, **Critical**.
- View the state of the finding, for example, **Active**.
- View the date and time at which the finding was last observed on the asset.
- View an icon representing the source application(s) the finding's asset originated from.

**Tip:** Hover over the icon to view the full application name.

- View the **Finding ID** associated with the finding.
- View the [VPR](#) of the finding.



**Tip:** Click [See in APA](#) to navigate directly to the [Top Attack Techniques](#) page automatically filtered by the selected finding.

- In the **Detection Timeline** section, view the following information about the finding:
  - **Last Seen** – The date on which the finding was last seen on an asset.
  - **First Seen** – The date on which the finding was first discovered on an asset.
  - **Last Updated** – The date on which the finding was last updated on the asset.
- View a brief **Solution** that describes how you can remediate the finding.
- View a list of **Properties** associated with the finding.

These can include, but are not limited to:

**Note:** The properties displayed in this section depend on the type of finding for which you are viewing details.

- **Finding ID** – The ID number associated with the finding.
- **Detection ID** – The ID number associated with the detection of the finding.
- **Active Finding Count** – The number of active findings on the asset.
- View a table list of the **Weaknesses** associated with the finding.

This list includes the following information:

- **Weakness Name** – The Common Vulnerability Exposure (CVE) ID associated with the weakness.
- **Type** – The type of weaknesses: **Misconfiguration** or **Vulnerability**.
- **Severity** – The severity of the weakness, for example, **Critical**.

**Note:** At this time, Tenable Exposure Management does not include information for Info level severity weaknesses.



**Note:** Because Tenable Exposure Management calculates CVEs using VPR and Tenable Cloud Security calculates using CVSS, you may notice a difference in severity across weaknesses between these applications.

- **VPR** – The [Vulnerability Priority Rating](#) (VPR) of the weakness.
- **Description** – A brief description of the weakness.
- **Impacted Assets** – The number of assets impacted by the weakness. For more information, see [Assets](#).
- **Sources** – The application the weakness' asset originated from, for example, Tenable Vulnerability Management.

## Software

The **Software** tab on the **Inventory** page highlights the installed software on your assets. Here, you can gain full visibility of the software deployed across your business and better understand the associated risks.

To access the **Software** tab:

1. Do one of the following:
  - In the left navigation menu, click **Inventory** > **Software**.
  - At the top of the [Inventory](#) page, click the **Software** tab.



The **Software** tab appears.

Assets 11.5kWeaknessesFindings 22.8kSoftware 234

Total Software Count234

New Software in Last 7 Days0

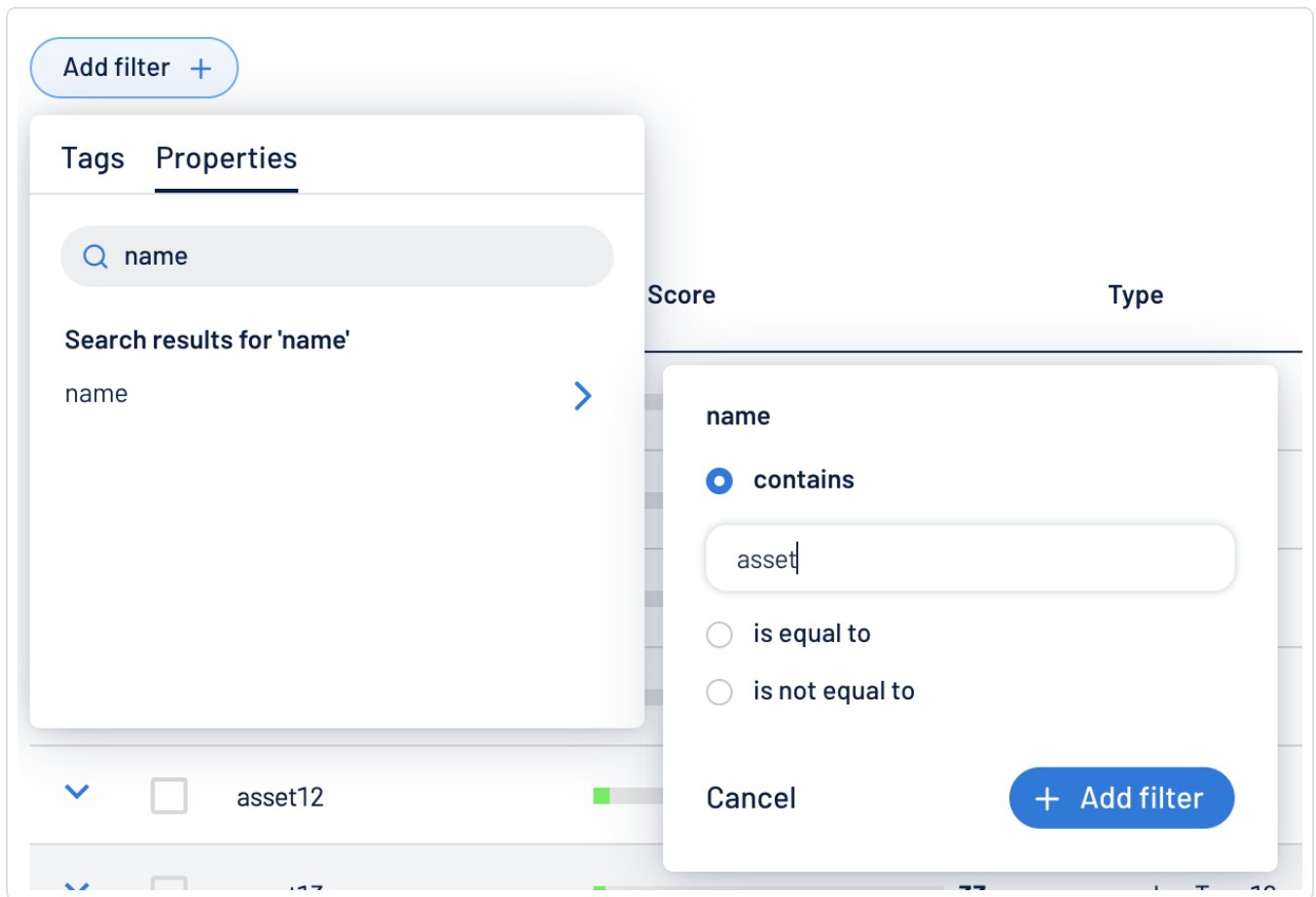
Software




Search for an application name or publisher...

Application	Publisher	Security End Of Life	Type	Version Count	Devices Count	Port Binding C...	File Location C...	Last Seen Version	Last Seen	See Details
<input type="checkbox"/> .Net Core	Microsoft	-	Application	4	2	0	4	1x 5.0.9	7 April 2024	See Details >
<input type="checkbox"/> .Net Core Windows	Any	-	Application	2	4	0	2	1x 6.0.2.3...	9 December 2023	See Details >
<input type="checkbox"/> .Net Framework	Microsoft	-	Application	22	77	0	24	1x 4.7.4115.0	26 February 2025	See Details >
<input type="checkbox"/> 7-Zip	7-Zip	-	Application	1	1	0	1	1x 21.6.0.0	7 April 2024	See Details >
<input type="checkbox"/> 7-Zip	Any	-	Application	4	6	0	2	1x 22.1.0.0	7 April 2024	See Details >
<input type="checkbox"/> Access	Microsoft	-	Application	4	5	0	3	1x 15.0.53...	7 April 2024	See Details >
<input type="checkbox"/> Acrobat Reader	Adobe	-	Application	2	4	0	2	1x 23.3.20...	7 April 2024	See Details >
<input type="checkbox"/> Adoptopenjdk Java	Any	-	Application	1	1	0	1	1x 1.8.0.27...	16 October 2023	See Details >
<input type="checkbox"/> Air	Adobe	-	Application	1	1	0	1	1x 3.7.0.20...	7 April 2024	See Details >
<input type="checkbox"/> Airflow	Apache	-	Application	27	171	13	1	1x unknown	15 November 2023	See Details >

On the **Software** tab, you can:

- View the total number of installed software applications on assets within your container.
- View the total number of new software applications discovered within the last 7 days.
- Use the **Search** box to search for a specific software application in the list.
- Filter the software list:



- a. Click the  button.  
The **Add filter**  button appears.
- b. Click **Add filter** .
- c. In the search box, type the criteria by which you want to search the list.  
Tenable Exposure Management populates a list of options based on your criteria.
- d. Click the property by which you want to filter the weakness list.  
A menu appears.



e. Select how to apply the filter. For example, if you want to search for a software application whose name includes *windows*, then select the **contains** radio button and in the text box, type *windows*.

f. Click **Add filter** .

The filter appears above the asset list.

g. Repeat these steps for each additional filter you want to apply.

h. Click **Apply filters**.

Tenable Exposure Management filters the list by the designated criteria.

- Export the table or the page:

a. (Optional) To export only specific table rows, in the table, select the check box next to the rows you want to export.

b. Click the  button.

The **Export** window appears.



## Export



### General

☐ Entire Table ☐ Current Page ☒ Selected Rows (3)

### File Name

Enter a name for the exported file.

### Formats

☒ CSV

☐ JSON

### Columns

Search columns

☒ 9 of 9 fields selected

[View selected](#)

☒ AES

☒ Asset Class

☒ Asset Name

☒ Associated Tags Count

☒ Last Update Date

Cancel

Export



c. Do one of the following:

- To export the entire table, select the **Entire Table** radio button.

**Note:** When you export the entire table, Tenable Exposure Management only includes the first 50 columns. To view asset data for a larger number of assets, use the [Search Assets API](#) call.

- To export the current page, select the **Current Page** radio button.
- To export the selected rows, select the **Selected Rows** radio button.

d. In the **File Name** text box, type a file name to give the exported file.

e. In the **Formats** section, select the format in which you want to export the data.

f. In the **Columns** section, select the check box for each column you want to include in the export file.

g. Click **Export**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.


- Customize the columns in the table:

a. Click **Columns** .

The **Customize columns** window appears.

b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.

c. (Optional) In the **Show/Hide** section, select/deselect the checkboxes to show or hide columns in the table.

d. (Optional) In the **Remove** section, click the  button to permanently remove a column from the table.

e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.





- i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

- ii. Select the checkbox next to any column or columns you want to add to the table.

- iii. Click **Add**.

The column appears in the **Customize columns** window.

- f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

- g. Click  **Apply Columns**.

Tenable Exposure Management saves your changes to the columns in the table.

- View a list of installed software, including the following information:

**Tip:** Click on any interactive number in the table to navigate directly to the [Software Details](#) view automatically filtered by the selected application and its related information.

- **Application** — The name of the software application installed on the asset.
- **Publisher** — The group or company that published the software application.
- **Security End of Life** — If applicable, the time frame after which the software becomes End of Life (EOL). After this date, no support or updates are provided for this software version, and users are encouraged to migrate to the latest version to ensure security and functionality.
- **Type** — The type of installed software, for example, **Application**.
- **Version Count** — The number of individual versions of the software detected on the asset.
- **Devices Count** — The number of individual devices with this software actively installed.
- **Port Binding Count** — The number of ports on the asset that are bound to the software application.
- **File Location Count** — The number of locations on your machine where the software application stores files.



- **Last Seen Version** – The version of the software that was most recently seen installed on an asset.
- **Last Seen** – The date and time at which the software was most recently seen on an asset.
- Click **See details** to view more details about a software application. For more information, see [Software Details](#).

## Software Details

In the **Software** view, you can view details for any software application in the list.

To view software details:

1. Access the [Software](#) view.
2. In the row of the software application for which you want to view details, click **See details**.

The software details page appears.

The screenshot shows the 'Software Details' page for 'OpenSSL'. At the top, there is a 'Back to Software Inventory' button. Below it, the software name 'OpenSSL' is displayed with a 'Last Seen' timestamp of 'Thursday 16 January 2025 at 03:30:22'. Two summary cards are shown: 'Devices' with a count of 3 and 'Number of Detected Versions' with a count of 3. Below these are tabs for 'Versions', 'Devices', 'File Locations', and 'Ports', with 'Versions' currently selected. A search bar is present above a table. The table has columns: 'Versions', 'Associated Devices', 'First Seen', 'Last Seen', 'Security End of Life', and 'Days On System'. It lists two versions of OpenSSL: 3.0.13 and 3.0.15, each with associated device counts, first/last seen dates, security end of life dates, and days on system.

Versions	Associated Devices	First Seen	Last Seen	Security End of Life	Days On System
3.0.13	3	March 31, 2024	January 16, 2025	1 Year	291
3.0.15	1	September 28, 2024	December 31, 2024	1 Year	94

On the software details page, you can:

- View the name and publisher of the software application.
- View the **Source** and the date and time at which the software **Last Seen** on an asset.



- View the total number of **Devices** impacted by the software application.
- View the **Number of Detected Versions** of the installed software.

When viewing the software details page, you can click on the following tabs to view additional asset information:

**Tip:** On any tab, use the **Search** box to further refine the software details.

## Versions

The **Versions** section shows a table list of each individual version of the software installed on your asset.

Versions				
Search...				
Search				
Versions	Associated Devices	First Seen	Last Seen ▾	Days On System
11.0.17763.6189	1	August 18, 2024	August 27, 2024	9
11.0.17763.5576	2	March 21, 2024	August 28, 2024	158

The list includes the following information:

- **Versions** – The version number of the installed software.
- **Associated Devices** – The number of assets that have this software application installed.
- **First Seen** – The date and time at which the software was first seen on an asset.
- **Last Seen** – The date and time at which the software was most recently seen on an asset.
- **Security End of Life** – If applicable, the time frame after which the software becomes End of Life (EOL). After this date, no support or updates are provided for this software version, and users are encouraged to migrate to the latest version to ensure security and functionality.
- **Days on System** – The number of days that the software has been installed on the asset.

## Devices

The **Devices** section shows a table list of the individual devices associated with the installed software.



Versions				
Devices				
File Locations				
Ports				
Search...				
Search				
Device Name ^	AES	Last Seen Version	Number of Versions	Last Seen
lucqa-afad-clie	<div><div></div></div> 598	<a href="#">4.7.4101.0</a>	4	August 27, 2024
lucqa-dc	-	<a href="#">4.7.4092.0</a>	3	August 26, 2024
lucqa-tools	-	<a href="#">4.7.4081.0</a>	2	August 26, 2024

The list includes the following information:

- **Device Name** – The name of the device on which the software is installed.
- **AES** – The overall [Asset Exposure Score](#) associated with the host.
- **Last Seen Version** – The most recent version of the software installed on the host.
- **Number of Versions** – The number of individual versions of the software installed on the host.
- **Last Seen** – The date and time at which the software was most recently seen on the host.

## File Locations

The **File Locations** section shows a table list of the locations on your machine where the software application stores files.

Versions		
Devices		
File Locations		
Ports		
Search...		
Search		
File Location ^	Version	Number of Hosts
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24030.9-0\	<a href="#">4.18.24030.9</a>	9
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24040.4-0\	<a href="#">4.18.24040.4</a>	8
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\	<a href="#">4.18.24050.7</a>	1

The list includes the following information:

- **File Location** – The file path of the location on your machine where the software application stores files.
- **Version** – The version number of the installed software associated with the file path.



- **Associated Devices** – The number of assets that have this software application version installed.

## Ports

The **Ports** section shows a table list of the locations on your machine where the software application stores files.

Versions   Devices   File Locations   Ports			
<input type="text" value="Search..."/> <span>Search</span>			
Port ^	Protocol	Version	Number of Devices
80	TCP	<span>ANY</span>	1

The list includes the following information:

- **Port** – The port number bound to the software application.
- **Protocol** – The protocol used to access the port, for example, **TCP**,
- **Version** – The version of the software that can use the port.
- **Number of Devices** – The number of devices that use this port.

## Dashboards

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The **Dashboards** page within Tenable Exposure Management offers built-in themed dashboards alongside customizable widgets, enabling seamless data exploration and full visibility across your Tenable One platform. This section includes with easy, on-demand export options that allow you to share at-a-glance views of key performance indicators (KPIs) relevant to a particular objective or business process.

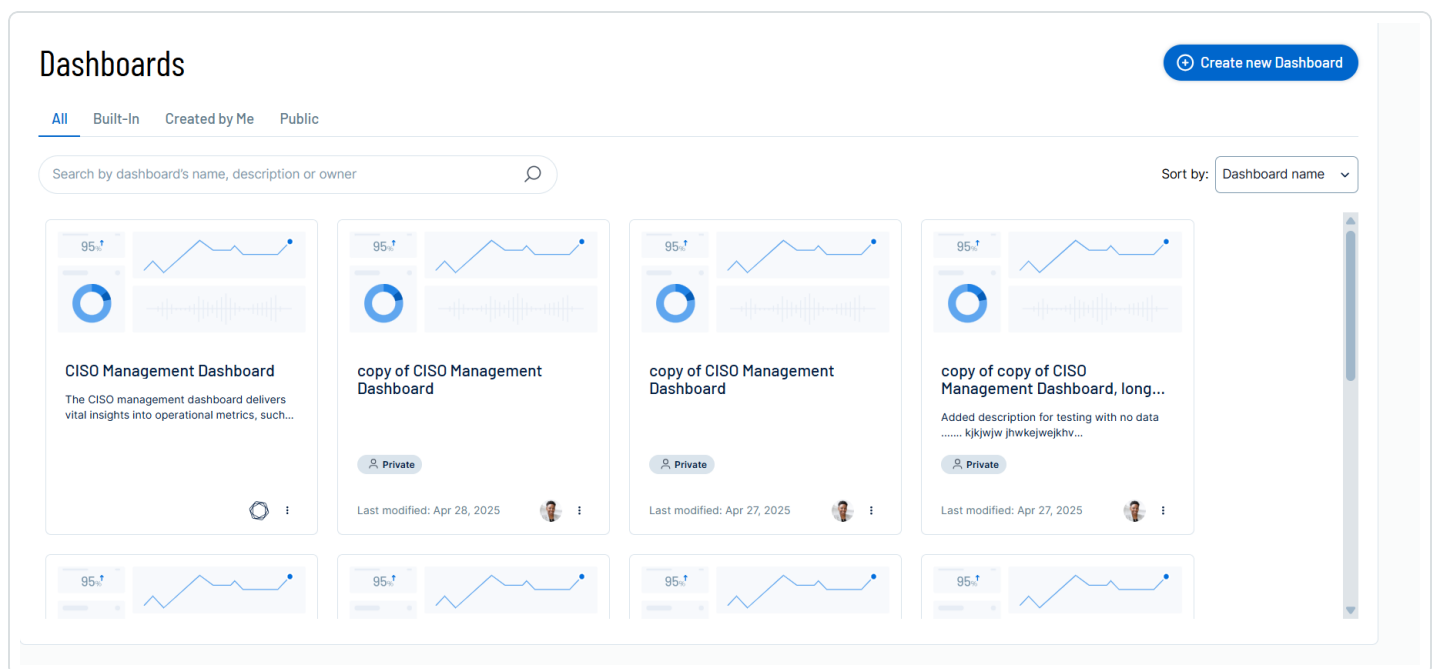
**Important:** Note the following dashboard limitations:

- Only licensed assets are included in dashboard data.
- By default, Tenable Exposure Management retains dashboard data within the user interface for 90 days. To access this data after this point, contact your Tenable representative.

- Dashboards only include data from [tags](#) created within Tenable Exposure Management. Dashboards do not include tag data from other Tenable applications or [third-party](#) sources.

The **Dashboards** page in Tenable Exposure Management separates your available dashboards into the following tabs:

- **All** – All dashboards available within your Tenable Exposure Management account.
- **Built-In** – Tenable-provided built-in dashboards that highlight common KPIs.
- **Created by Me** – All dashboards created by you.
- **Public** – All public dashboards created by users within your Tenable Exposure Management container.



**Note:** Tenable refreshes dashboard data daily at 3:00 AM in the time zone within which the container resides.

To access the **Dashboards** page:

1. In the left navigation menu, click **Analytics**.

A menu appears.



## 2. Click **Dashboards**.

The **Dashboards** page appears.

On each tab, you can view tiles that represent your available dashboards.

You can modify the list of tiles in the following ways:

- Use the search bar to search for a dashboard by its name, description, or owner.
- In the upper-right corner of the list, from the Sort by drop-down menu, select how you want to sort the list of dashboard tiles:
  - **Modification Date**
  - **Dashboard Name**

On each tile, you can:

**Note:** If a tile shows **(Blank)**, this means Tenable Exposure Management cannot find data for the tile. This may mean no data is available for the tile or a dashboard filter is hiding the tile's data.

- View the title of the dashboard.
- View an icon that represents the owner of the dashboard.
- Create a copy of the dashboard:

- a. Click the  button.

A menu appears.

- b. Click  **Create a Copy**.

The **Create a copy** window appears.

## Create a copy


**Dashboard Name** \*

copy of SLA Tracking Dashboard

**Description**

The SLA tracking dashboard offers comprehensive visibility into the overall status and progress of SLAs across your organization and per each Assets groups (Tags). It is entirely driven by the established SLA policies, which provide clear, measurable benchmarks for monitoring and evaluating vulnerability remediation efforts. SLA policies act as defined targets or

0 / 200



**Private Dashboard**  
This dashboard is currently private . Toggle on to set as public.

☐

Cancel

Create

- c. In the **Dashboard Name** text box, type a name for the copied dashboard. By default, Tenable prepends "copy of" to the original dashboard name.
- d. (Optional) In the **Description** text box, edit the dashboard description.
- e. In the dashboard privacy section, select whether you want the dashboard to be **Public** or **Private**.

**Note:** Public dashboards are visible to all users within your Tenable Exposure Management instance.

- Click on a dashboard tile to view additional [dashboard details](#).

Additionally, you can manage your dashboards in the following ways:





- [Create](#) a new dashboard.
- [Edit](#) a custom dashboard.
- [Change](#) the privacy of a custom dashboard.
- [Delete](#) a custom dashboard.

## Dashboard Overview

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

You can drill into any dashboard on the [Dashboards](#) page to view the dashboard's overview.

**Important:** Note the following dashboard limitations:

- Only licensed assets are included in dashboard data.
- By default, Tenable Exposure Management retains dashboard data within the user interface for 90 days. To access this data after this point, contact your Tenable representative.
- Dashboards only include data from [tags](#) created within Tenable Exposure Management. Dashboards do not include tag data from other Tenable applications or [third-party](#) sources.

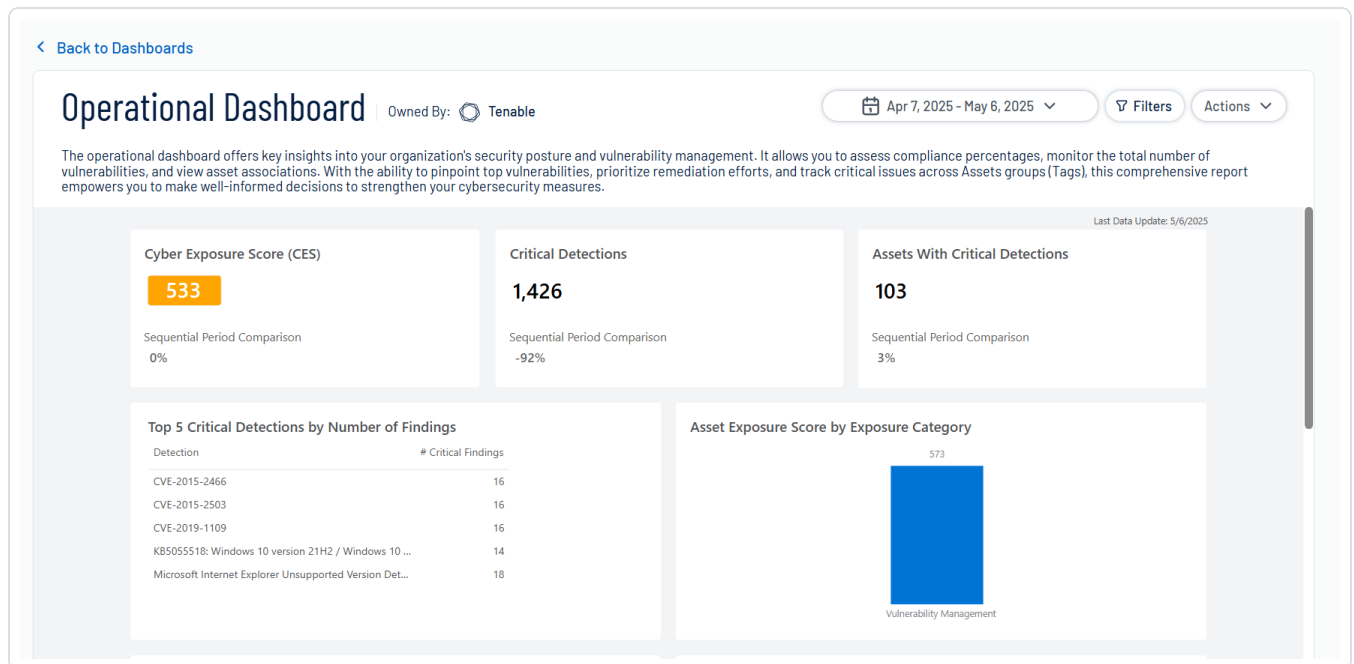
**Note:** Tenable refreshes dashboard data daily at 3:00 AM in the time zone within which the container resides.

To view a dashboard overview:

1. Access the [Dashboards](#) page.
2. Click the tile of the dashboard for which you want to view the overview.



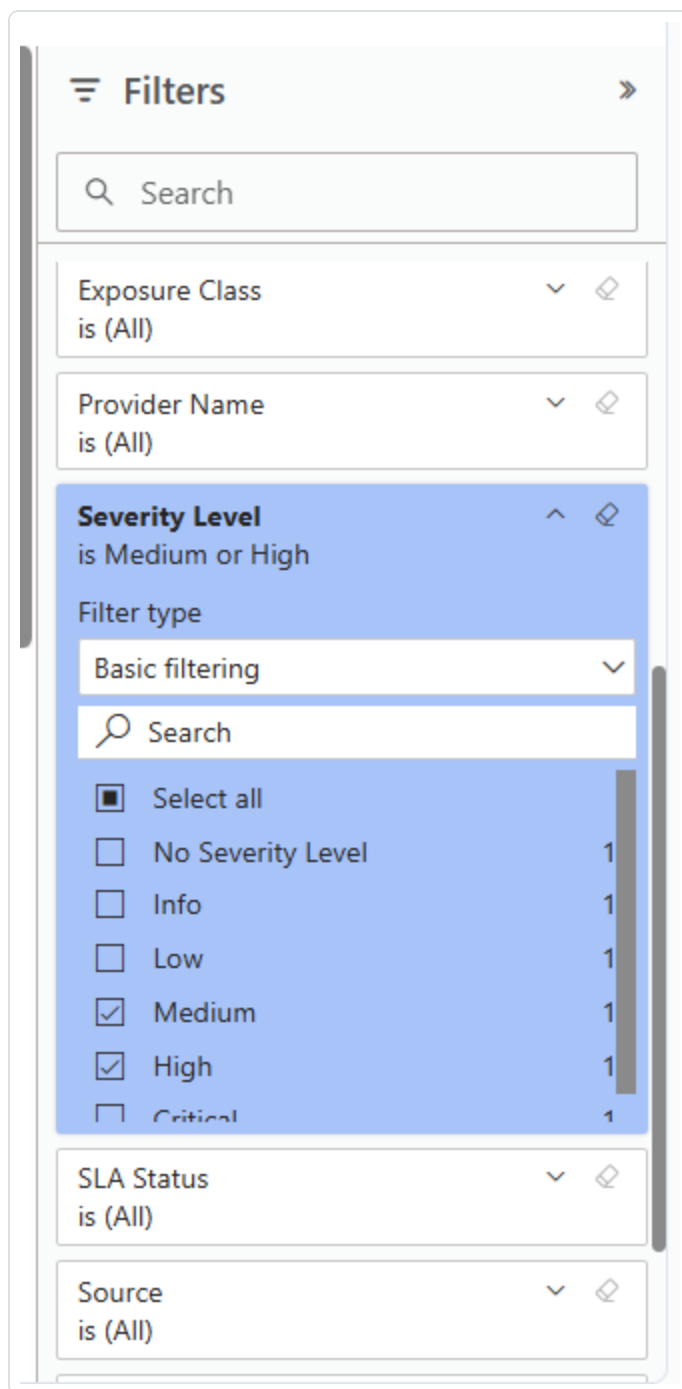
The dashboard overview appears.



On the dashboard overview page, you can:

- View the dashboard's name.
- View the owner of the dashboard.
- In the upper-right corner, use the date range drop-down to select the date range for which you want to view data on the dashboard.
- Click the **Filters** button to apply one or more filters to the dashboard overview.

The **Filters** pane appears.



- a. Expand any filter drop-down to apply filters of that type. For example, expand the **Asset Type** drop-down to filter the dashboard overview by a specific type of asset.



**Tip:** Tenable Exposure Management groups filters based on whether they are applied to the whole dashboard or an individual widget. Applied filters appear in blue, so you can easily identify which filters are currently affecting your dashboard and widget data.

- Expand the **Actions** drop-down to view dashboard options:

- **Export** — Click to export the dashboard for sharing:

A menu appears.

- a. Select the format in which you want to export the dashboard.

Tenable Exposure Management sends the exported file to your customer email address.

- **Create a Copy** — Click to create a copy of the dashboard:

The **Create a copy** window appears.

- a. In the **Dashboard Name** text box, type a name for the copied dashboard. By default, Tenable prepends "copy of" to the original dashboard name.
- b. (Optional) In the **Description** text box, edit the dashboard description.
- c. In the dashboard privacy section, select whether you want the dashboard to be **Public** or **Private**.

**Note:** Public dashboards are visible to all users within your Tenable Exposure Management instance.

- d. Click **Create**.

Tenable Exposure Management adds the copy of the dashboard to the [Dashboards](#) page.

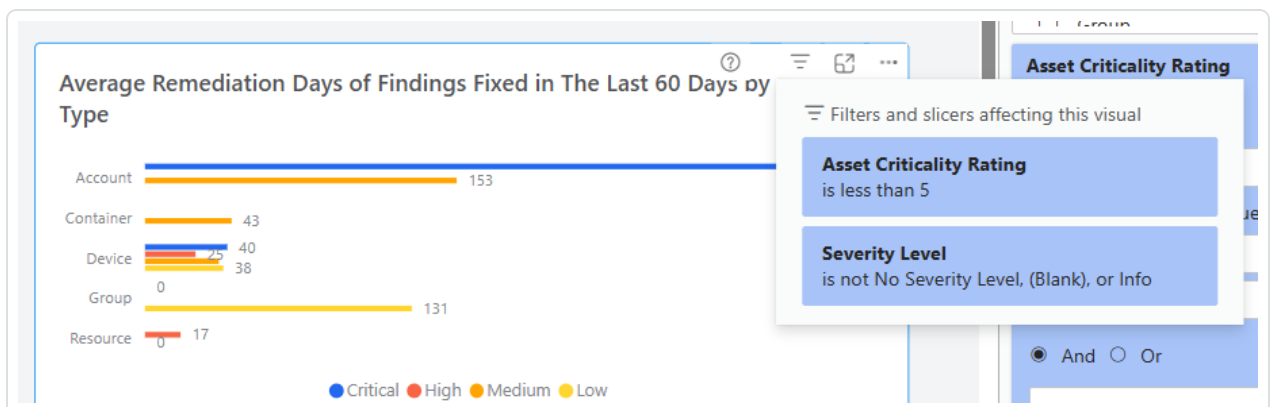
- View details about the widgets within your dashboard. The data on each widget depends on the type of widget and the configurations applied during creation.

In the upper-right corner of each widget, you can interact with and manage your dashboard's widgets. These options include, but are not limited to:



**Note:** The widget management options depend on the type of widget you're managing. Not all widget types include these options.

- Hover over the button to view a brief description of the data on the widget.
- If you've drilled down into a specific data point, click the button to drill back up to the main data within the widget.
- If you're at the top level of widget data, click the button to turn on drill down mode. Once on, you can click a data point on the graph to drill down into that specific data point for more detailed information.
- Click the button to drill down to the lowest level of data available on the widget.
- Click the button to view additional options for viewing and exporting widget data.
- Click the filter button to view all filters affecting the widget:



## Manage Dashboards

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

In Tenable Exposure Management, you can manage dashboards in the following ways:

### Create a Dashboard

In Tenable Exposure Management, you can create a dashboard to highlight key performance indicators (KPIs) for yourself and others within your organization.

To create a new dashboard:



1. At the top of the [Dashboards](#) page, click the **+ Create New Dashboard** button.

The create dashboard page appears.

2. In the **Dashboard Name** text box, type a name for the dashboard.
3. (Optional) To add a description to the dashboard, click the button.

A text box appears.

- a. In the **Dashboard Description** text box, type a brief description of the dashboard.
  - b. Click the button to save the description.
4. From the date range drop-down, select the date range for which you want to view data on the dashboard.

**Tip:** Choose a **Quick** pre-defined date range, or select your own date range on the **Custom** tab.

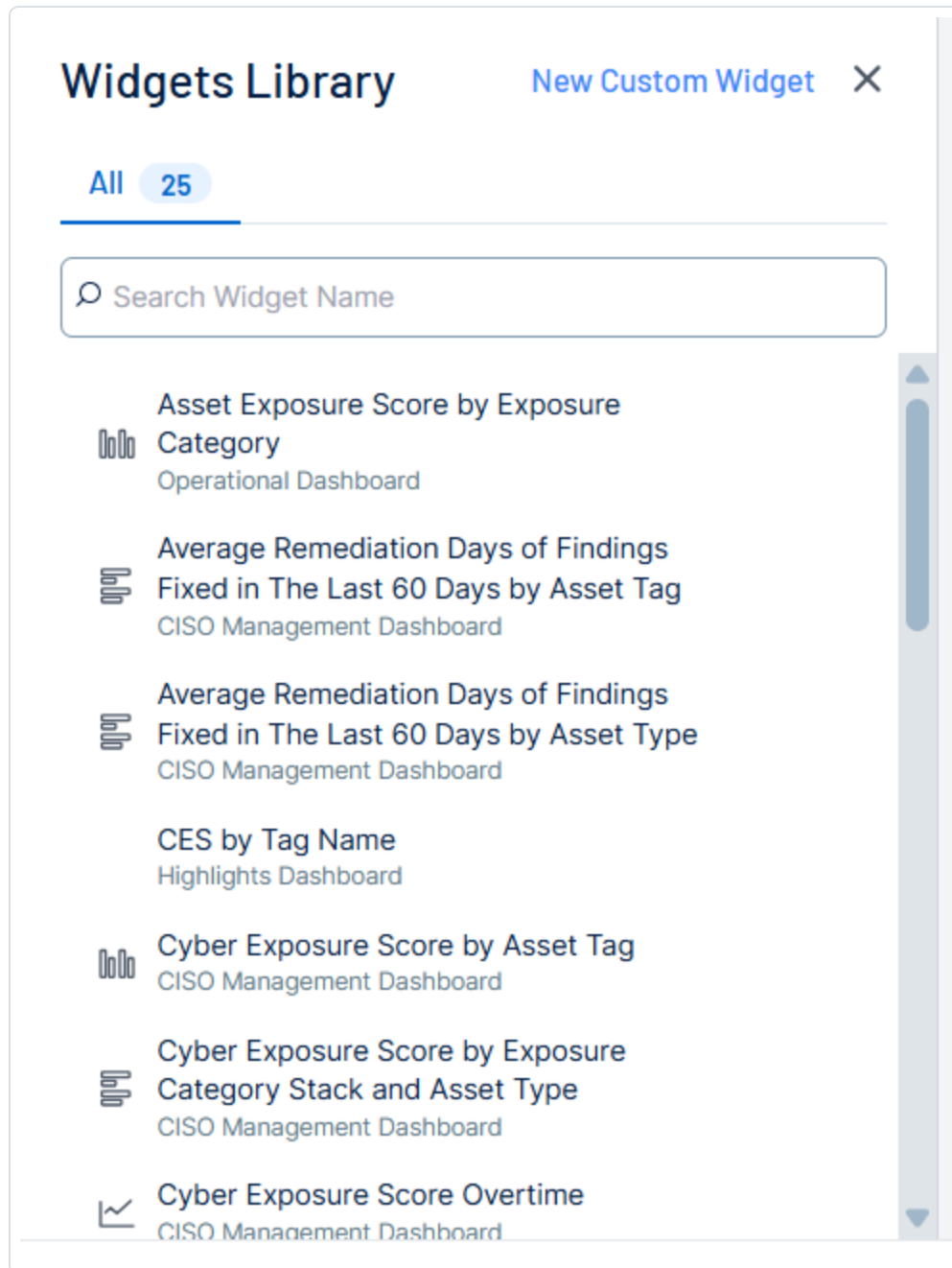
5. (Optional) Click the **Filters** button to apply one or more filters to the dashboard.

**Note:** This filter applies to all individual widget data on the dashboard.

6. Add widgets to the dashboard:


- a. On the create dashboard page, click **+ Add Widgets**.

The **Widgets Library** appears.



- b. Do one of the following:



- Select a widget from the **Widgets Library**:
    - i. In the **Widgets Library**, for the widget you want to add to the dashboard, click the  button.
- Tip:** Use the search box to search for a specific widget in the library.
- The widget appears in the dashboard preview pane.
- ii. Repeat for each widget you want to add from the **Widgets Library**.
- Create a new custom widget:
  - i. In the upper-right corner of the **Widgets Library**, click **New Custom Widget**.
- The **Custom Widget** pane appears.





←

## Custom Widget

×

Widget Name \*

Widget Type

Table ▼

Table Columns \*

Select ▼

Chart Filters

[🔗 Apply Widget Filters](#)

No Filters Applied

Save

- ii. In the **Widget Name** text box, type a name for the custom widget.
- iii. From the **Widget Type** drop-down, select the type of data graph you want to use on the widget, for example, **Pie Chart** or **Table**.




The custom widget configuration options update depending on the type of data graph you select.

- iv. Configure the data according to your preferences. For example, if you select **Scatter Chart**, you can configure the **Values**, **X axis**, **Y axis**, and **Legend** for the chart.

The widget updates automatically within the dashboard preview.

**Important!** For information on what values and fields you can configure based on your chart selection, see [Valid Custom Widget Combinations](#).

- v. (Optional) In the **Chart Filters** section, to apply filters to the data within the custom widget, click  **Apply Widget Filters**.

**Note:** This filter only applies to the data within this custom widget.

- vi. Click **Save**.

- c. Click **Create**.

The **Dashboard Details** window appears.


- d. In the **Private Dashboard** section, enable or disable the toggle to set the dashboard as **Public** or **Private**.

**Note:** Public dashboards can be seen by all users within your Tenable Exposure Management container.

## Copy a Dashboard

In Tenable Exposure Management, you can make a copy of any dashboard on the [Dashboards](#) page.

To copy a dashboard:

1. Do one of the following:
  - On the [Dashboards](#) page, in the lower-right corner of the tile for the dashboard you want to copy, click the  button.



- On the [dashboard details](#) page, in the upper-right corner, expand the **Actions** drop-down.

A menu appears.

2. Click  **Create a Copy**.

The **Create a copy** window appears.


## Create a copy

**Dashboard Name \***

**Description**


The SLA tracking dashboard offers comprehensive visibility into the overall status and progress of SLAs across your organization and per each Assets groups (Tags). It is entirely driven by the established SLA policies, which provide clear, measurable benchmarks for monitoring and evaluating vulnerability remediation efforts. SLA policies act as defined targets or

0 / 200



**Private Dashboard**

This dashboard is currently private . Toggle on to set as public.



Cancel

Create

3. In the **Dashboard Name** text box, type a name for the copied dashboard. By default, Tenable prepends "copy of" to the original dashboard name.
4. (Optional) In the **Description** text box, edit the dashboard description.



5. In the dashboard privacy section, select whether you want the dashboard to be **Public** or **Private**.

**Note:** Public dashboards are visible to all users within your Tenable Exposure Management instance.

6. Click **Create**.

Tenable Exposure Management adds the copy of the dashboard to the [Dashboards](#) page.


### Edit a Custom Dashboard

**Note:** Only the dashboard owner can perform this action.

In Tenable Exposure Management, you can edit custom dashboards by either quick-editing their name and description, or accessing the **Edit Dashboard** page to fully edit the dashboard's configuration options.

**Note:** You cannot edit Tenable provided dashboards.


To edit a custom dashboard's name and/or description:

1. On the [Dashboards](#) page, in the lower-right corner of the tile for the custom dashboard you want to edit, click the  button.

A menu appears.

2. Click  **Edit Name or Description**.

The **Dashboard Details** window appears.




## Dashboard Details ✕

**Dashboard Name \***

**Description**

Add a description here

0 / 200


 **Public Dashboard** This dashboard is currently public . Toggle off to set as private. ☒

Cancel Update

3. Edit the **Dashboard Name** and/or **Description**.
4. (Optional) Edit the dashboard's privacy (for example, **Public** or **Private**).
5. Click **Update**.



Tenable Exposure Management saves your changes to the dashboard.

To edit a custom dashboard via the **Edit Dashboard** page:

1. Do one of the following:
  - On the [Dashboards](#) page, in the lower-right corner of the tile for the custom dashboard you want to edit, click the  button.



A menu appears.

- a. Click  **Edit Dashboard**.
- On the [dashboard details](#) page for the custom dashboard, in the upper-right corner, click  **Edit Dashboard**.

The edit dashboard page appears.

2. Make any desired changes to the dashboard. For more information about the dashboard configuration options, see [Create a Dashboard](#).
3. Click **Update**.

Tenable Exposure Management saves your changes to the dashboard.


## Change the Privacy of a Custom Dashboard

**Note:** Only the dashboard owner can perform this action.



You can set the privacy of custom dashboards to either **Public** or **Private**.

**Note:** You cannot delete Tenable provided dashboards.

To change the privacy of a custom dashboard:

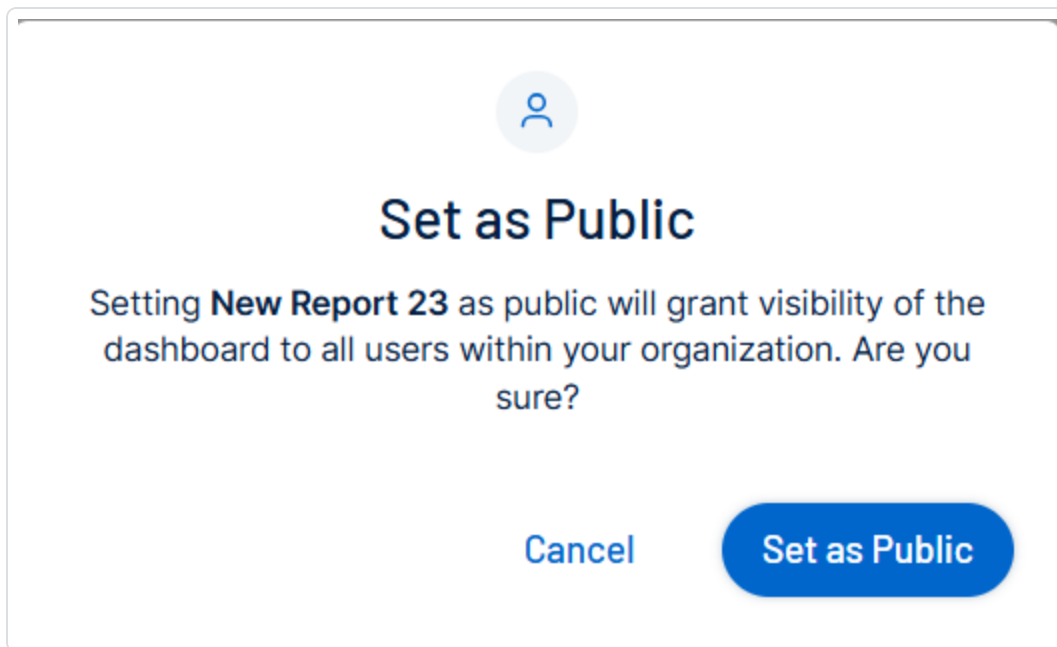
1. Do one of the following:
  - On the [Dashboards](#) page, in the lower-right corner of the tile for the custom dashboard you want to copy, click the  button.
  - On the [dashboard details](#) page for the custom dashboard, in the upper-right corner, expand the **Actions** drop-down.

A menu appears.

2. Do one of the following:
  - If the dashboard is currently private, click  **Set as Public**.
  - If the dashboard is currently public, click  **Set as Private**.

A confirmation message appears.

3. Click **Set as Public/Private**.



Tenable Exposure Management updates the privacy of the selected dashboard.


## Delete a Custom Dashboard

**Note:** Only the dashboard owner can perform this action.

In Tenable Exposure Management, you can delete custom dashboards.

**Note:** You cannot delete Tenable provided dashboards.

To delete a custom dashboard:

1. Do one of the following:
  - On the [Dashboards](#) page, in the lower-right corner of the tile for the custom dashboard you want to delete, click the  button.
  - On the [dashboard details](#) page for the custom dashboard, in the upper-right corner, expand the **Actions** drop-down.

A menu appears.

2. Click  **Delete Dashboard**.



A confirmation message appears.

3. Click **Delete Dashboard**.

Tenable Exposure Management removes the dashboard and its data from the user interface.

## Valid Custom Widget Combinations

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

When creating a custom widget in the **Analytics** > [Dashboards](#) section, Tenable Exposure Management performs a data validation check to ensure all optional chart data combinations work together. When you choose an option, other options are filtered so show only items that have a relationship with your chosen option.

The tables below highlight the valid possible data combinations for all widget types within Tenable Exposure Management.

## Table Relationships

Source Table	Related Tables
DimAsset	FactAsset, FactFinding
DimDate	FactAsset, FactDetection
DimDetection	FactDetection, FactFinding
DimExposureClass	FactAsset, FactFinding
DimGroupTag	FactAsset, FactFinding
DimSeverity	FactAsset, FactDetection, FactFinding
DimSLAStatus	FactAsset
DimSource	FactAsset, FactFinding
FactAsset	DimAsset, DimDate, DimExposureClass, DimGroupTag, DimSeverity, DimSLAStatus, DimSource





FactDetection	DimDate, DimDetection, DimSeverity
FactFinding	DimAsset, DimDetection, DimExposureClass, DimGroupTag, DimSeverity, DimSource

## Drop-down Relationships

Display Name	Table
Asset Criticality Rating	DimAsset
Asset Class	
Asset Name	
Asset Creation Date	
Asset Disabled Date	
Asset First Observation Date	
Asset Last Licensed Date	
Asset Last Observed Date	
Asset Last Updated Date	
License Expires	
Provider Name	



Date	DimDates
Day of Month	
Day of Year	
Month Name in Year	
Quarter	
Quarter in Year	
Week Day Name (Short)	
Year	
Month in Year	
First Date of Month	
First Date of Quarter	
First Date of Week	
First Date of Year	
Detection Name	DimDetection
VPR Score	
Exposure Category	DimExposureClass
Tag Name	DimGroupTag
Severity	DimSeverity
SLA Status	DimSLAStatus
Asset Source	DimSource



# Assets	FactAsset
# Compliant Assets	
Average CES	
# Breaching Assets	
Average AES	
# Total Findings (by asset)	
# Active Findings (by asset)	
# Fixed Findings (by asset)	
# Resurfaced Findings (by asset)	
# Detections	FactDetection
# Active Findings (by detection)	
# Findings - Current	FactFinding
# Breaching Findings - Current	
# Compliant Findings - Current	
# Findings Approaching SLA - Current	
# High Critical Findings Approaching SLA - Current	
# High Critical Breaching Findings - Current	
Average Remediation Days - Current	
Average Breaching Days - Current	
SLA Breaching Findings - Current	
SLA Compliant Findings - Current	
# Critical Findings - Current	
Finding State	



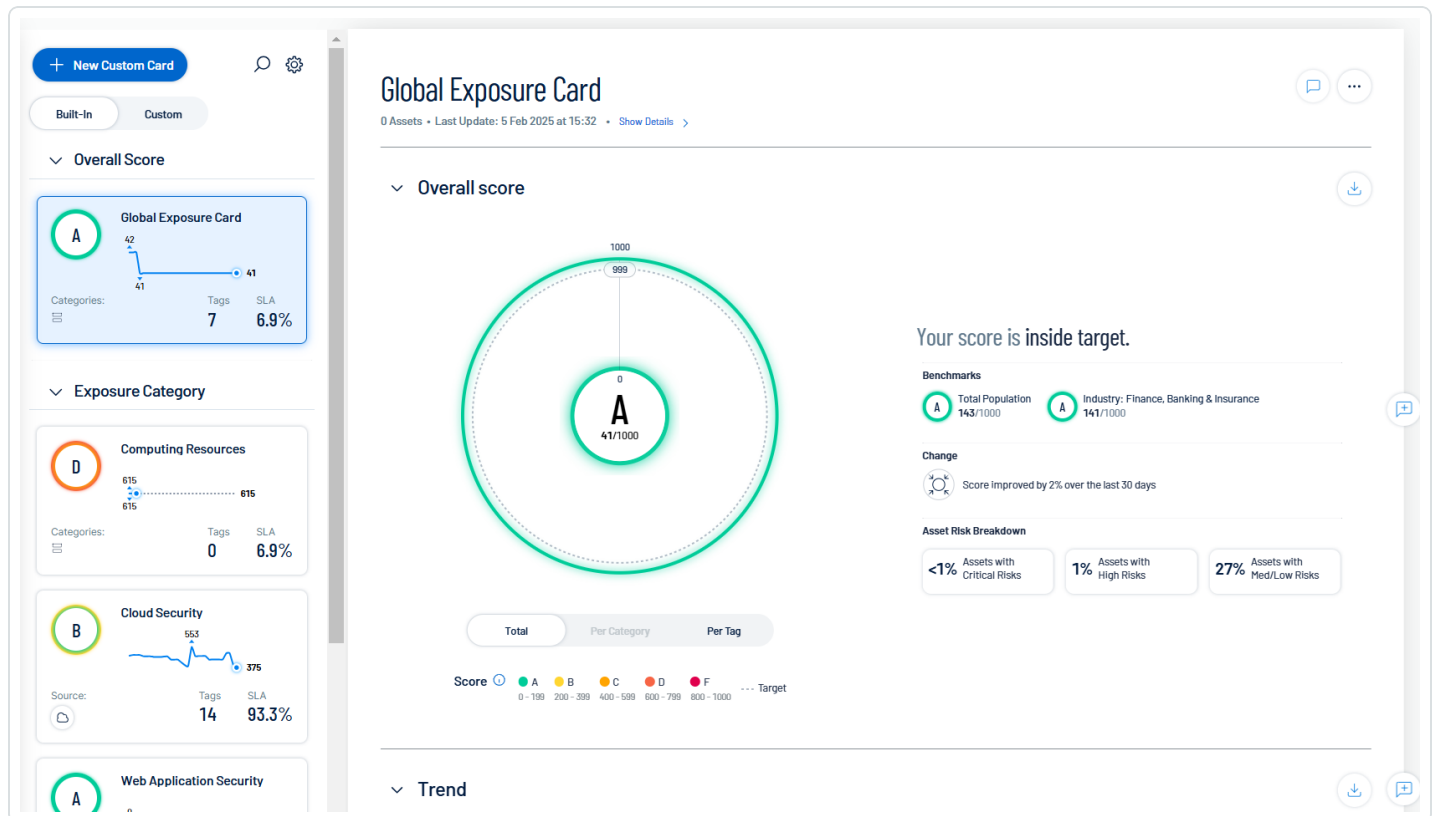
## Exposure View

The **Exposure View** page in Tenable Exposure Management allows you to quickly view your global CES, see its changes and trends over time, view important benchmark comparisons, and assess your overall risk. The **Exposure View** page includes several tools that help you understand:

- Your overall security posture as it relates your business context
- The criticality of your assets
- The effectiveness of your efforts to remediate vulnerabilities across your workspace

An exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your Cyber Exposure Score (CES) and other metrics. Users can create custom cards, or use Tenable-provided cards to gain insight and guidance on what areas need their attention most.

**Note:** Because exposure card scores are globally calculated, [role-based access control](#) (RBAC) does not affect card data on the **Exposure View** page.



To access the **Exposure View** page:



1. In the left navigation menu, click **Exposure View**.

A menu appears.

2. Click **Dashboards**.

The **Exposure View** page appears.

The **Exposure View** page includes the following sections:

### Exposure Card Library

An exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your Cyber Exposure Score (CES) and other metrics. Users can create custom cards, or use Tenable-provided cards to gain insight and guidance on what areas need their attention most.

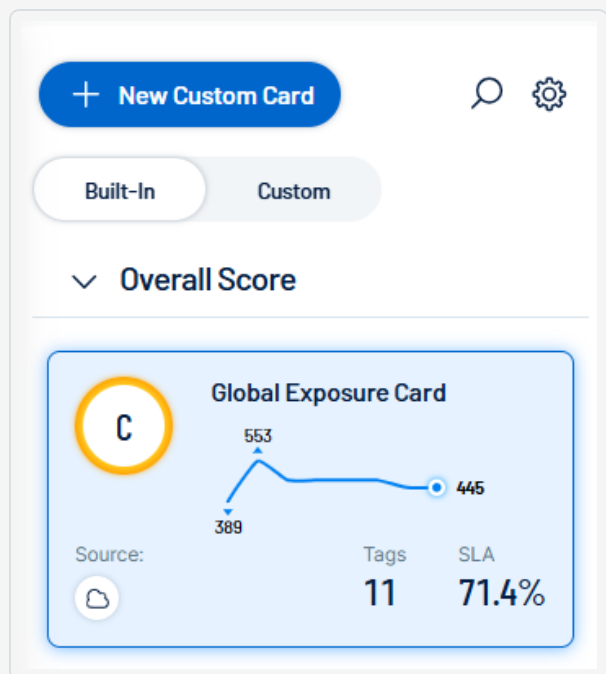
**Tip:** For more information on managing exposure cards, see [Manage Exposure Cards](#).

**Note:** Because exposure card scores are globally calculated, [role-based access control](#) (RBAC) does not affect card data on the **Exposure View** page.

The exposure card library on the left side of the **Exposure View** page allows you to interact with the following types of exposure cards:

Card type	UI Image
<b>Built-in</b> Tab	

A Tenable-provided **Global Exposure Card** that shows your **Overall Score** based on all internal and external data within Tenable Exposure Management.



Tenable-provided **Exposure Category** cards based on data from the following categories:

- **Web Application Security** – All data from Tenable Web App Scanning sources.
- **Identity Exposure** – All data from Tenable Identity Exposure sources.

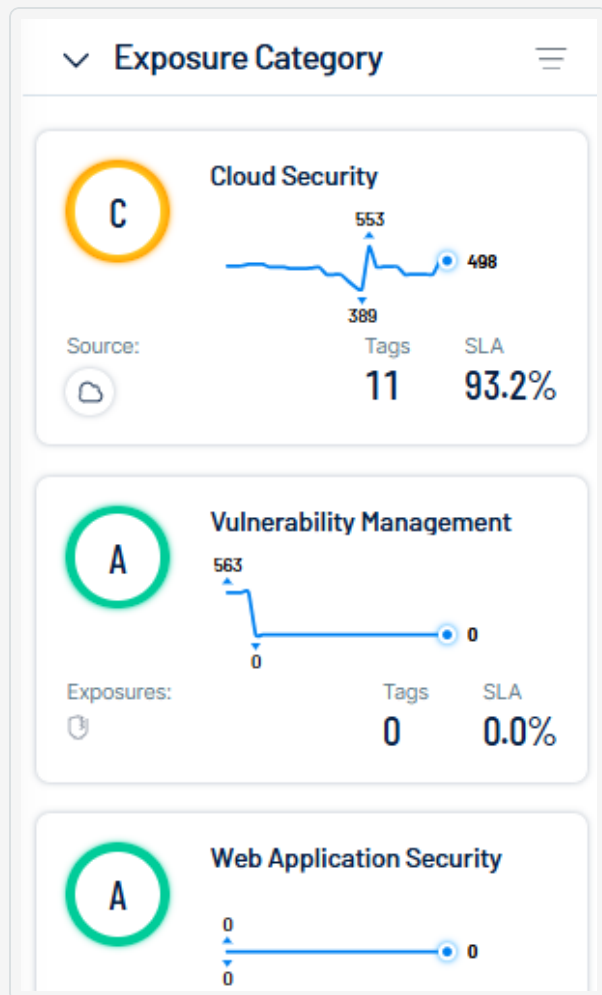
**Important:** The **Identity Exposure** card is only visible if you've [enabled the Use the Tenable Cloud Service option](#) in Tenable Identity Exposure.

- **Vulnerability Management** – All data from Tenable Vulnerability Management sources.

**Note:** Data from third party applications appears on the Vulnerability Management exposure card. For more information, see [Data Sources](#).

- **Cloud Security** – All data from Tenable Cloud Security sources.
- **Operational Technology** – All data from Tenable OT Security sources.

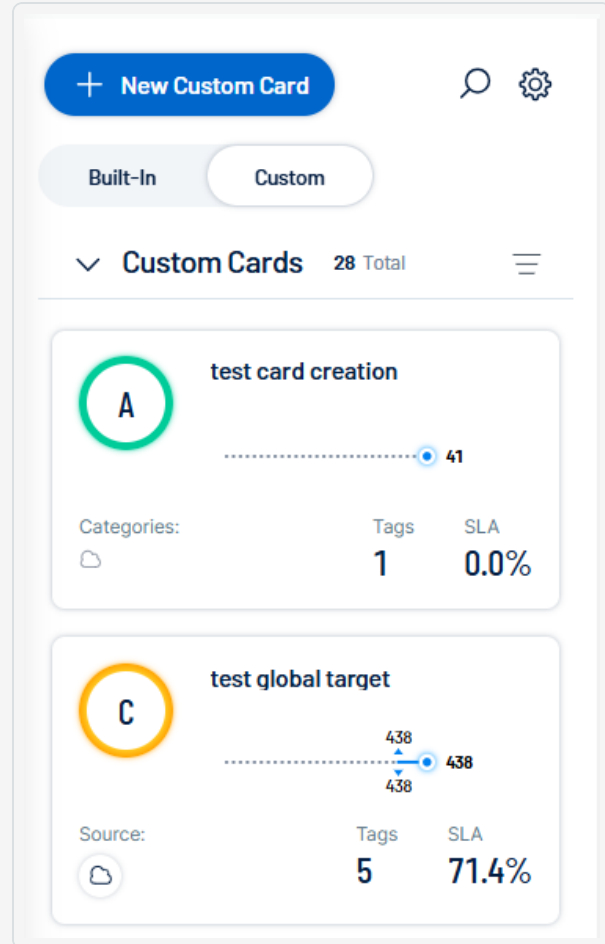
**Note:** The widgets and data on each card are determined by the type of data within each category.



**Custom Tab**

Data from user-created [user-created](#) custom exposure cards.

For more information, see [Manage Exposure Cards](#).



## General Exposure Card Data

At the top of the **Exposure View**, you can view and manage the card data that appears within the **Exposure View**.

Here, you can:

- In the upper-left corner of the page, view the time at which Tenable Exposure Management last updated the CES.
- In the upper-left corner of the page, view the [sources](#) whose data is calculated as part of the exposure card.
- In the upper-left corner of the page, click **Show Details** to view the following exposure card information:



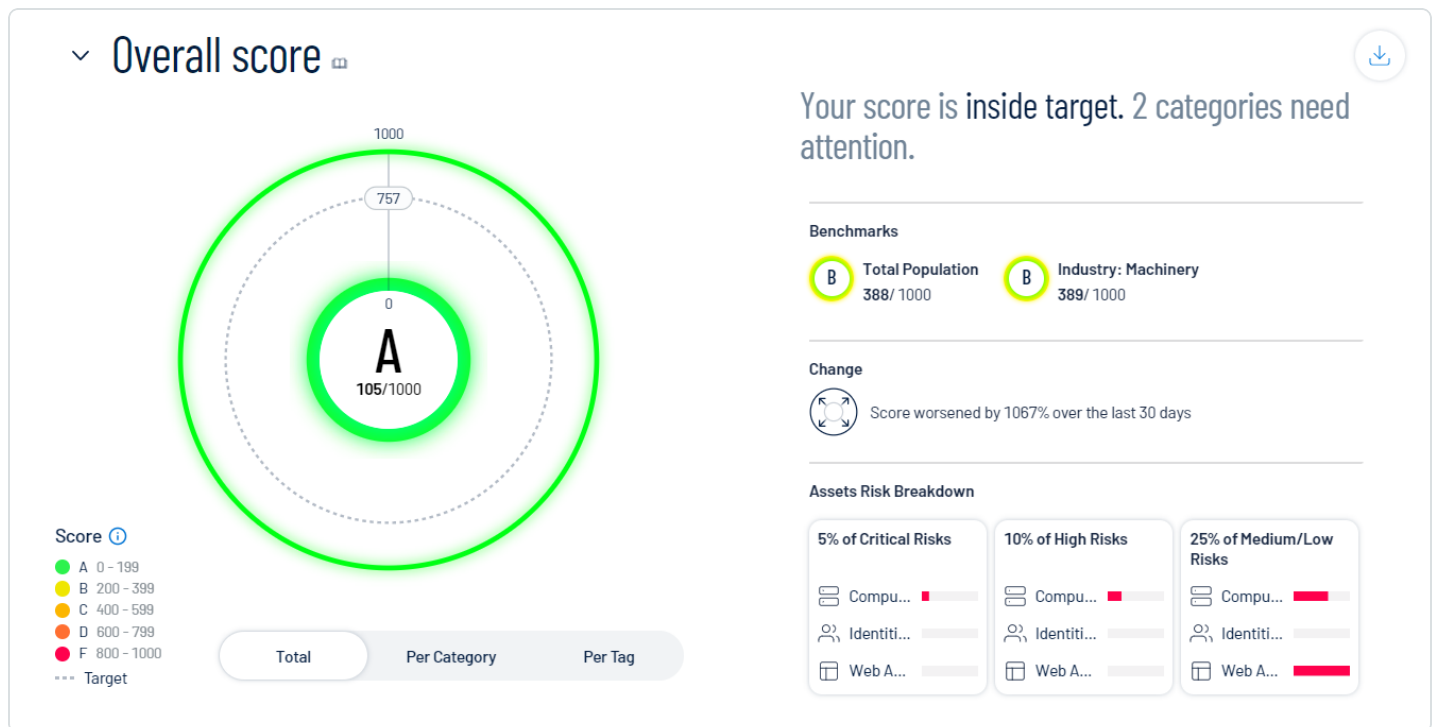
- **Card Info**, such as the user that created the exposure card, and the date and time at which the exposure card was created.
- A full list of the data **Tenable Data Sources** whose data is calculated as part of the exposure card.

## CES

By default, the **Exposure View** page displays your **Global** Cyber Exposure Score. You can select a specific card via the [exposure card library](#) to view your Cyber Exposure Score for that card. CES data is available for the following categories:

- Tenable-provided exposure cards.
- Data from user-created [custom](#) exposure cards.

**Note:** Because exposure card scores are globally calculated, [role-based access control](#) (RBAC) does not affect card data on the **Exposure View** page.



**Note:** Tenable Exposure Management does not include assets older than 90 days in your CES.

To view your CES for an exposure card:



1. In the [exposure card library](#), select the exposure card for which you want to view your CES.

The **Exposure View** page displays CES details for the selected card.

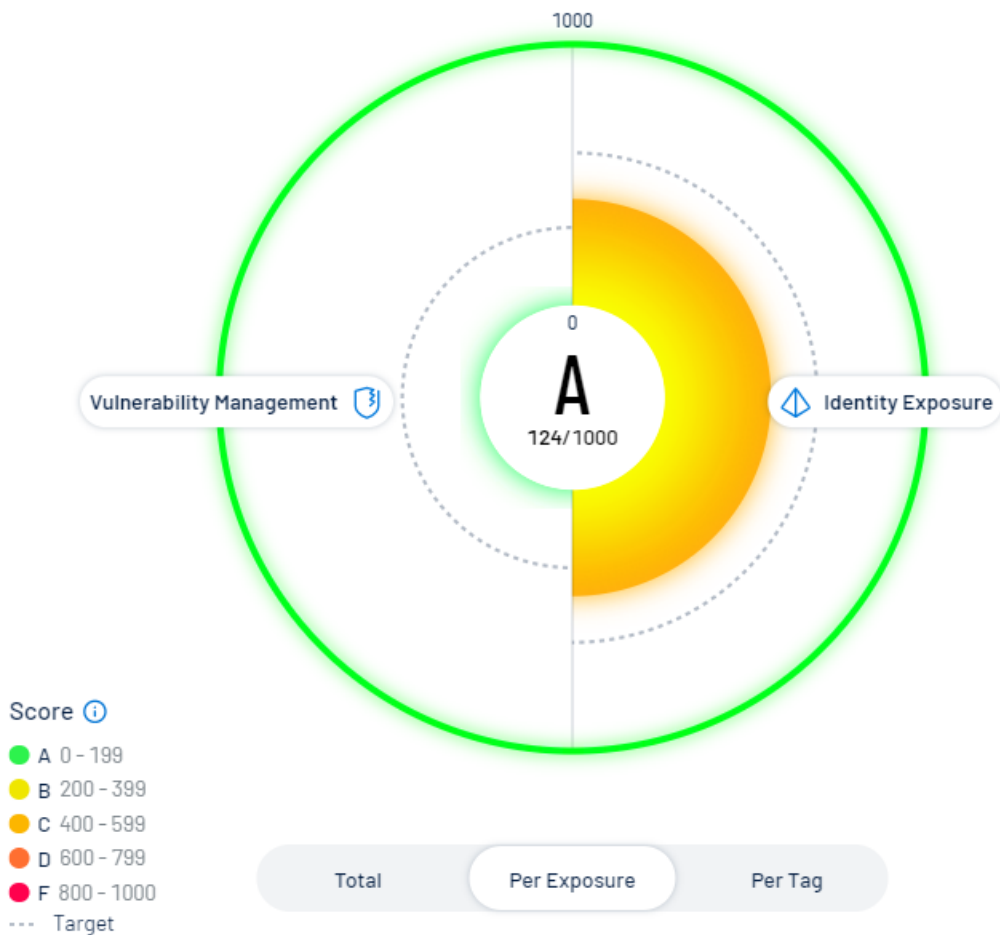
While viewing the CES details for a card, you can:

- View a graphical representation of your CES grade as it compares to your industry and the total population:
  - To view your total CES regardless of the data source, below the circle graph, click **Total**.
  - To view your CES separated based on the source of the exposure, below the circle graph, click **Per Exposure**.

The CES graph splits into sections that represent each exposure source, for example, **Identity Exposure**. For more information, see [Tenable Exposure Management Metrics](#).

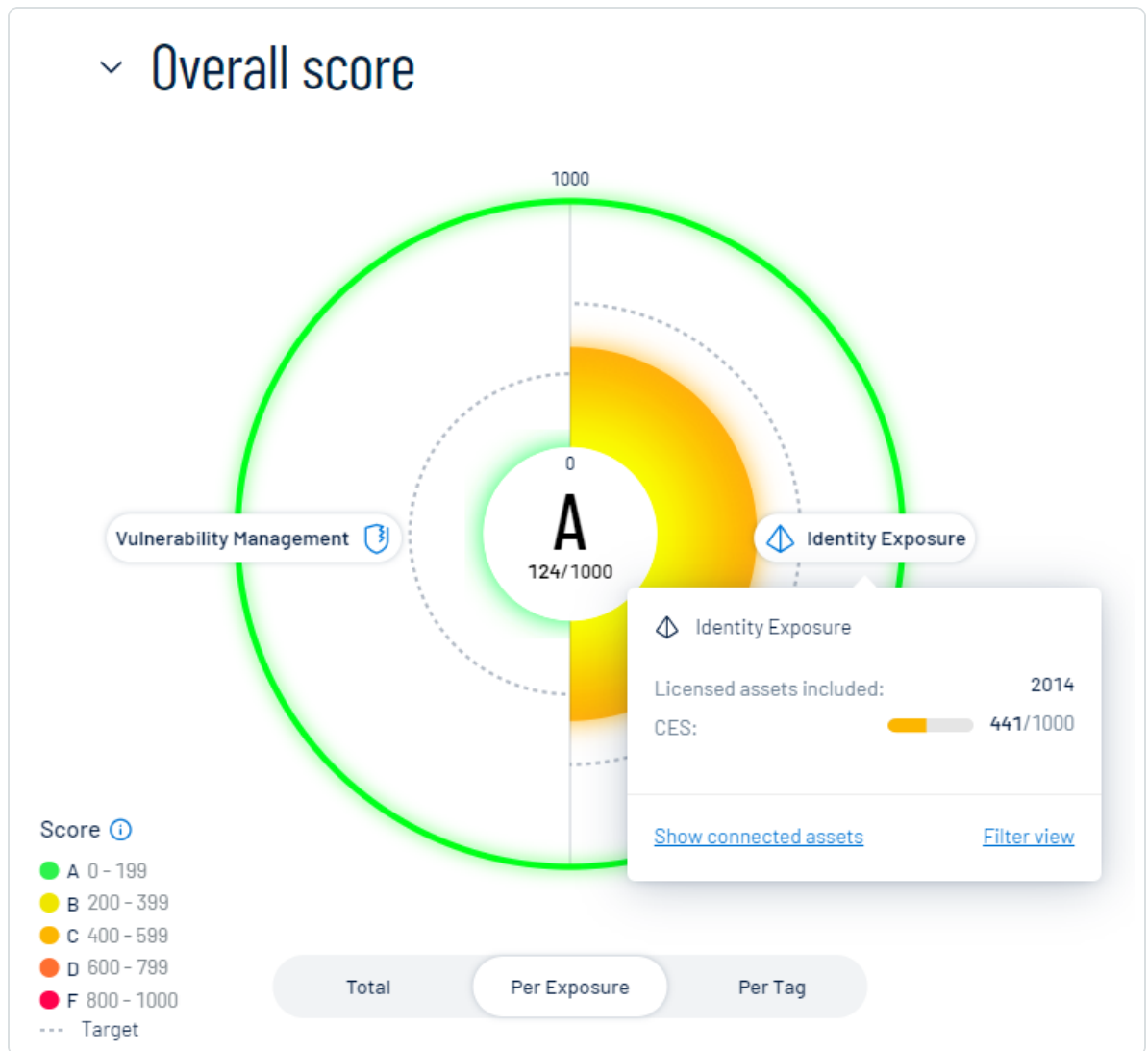


## Overall score



- Within the CES graph, click an individual category name to view additional category information, [connected assets](#), and to filter the **Exposure View** page by

the selected category.



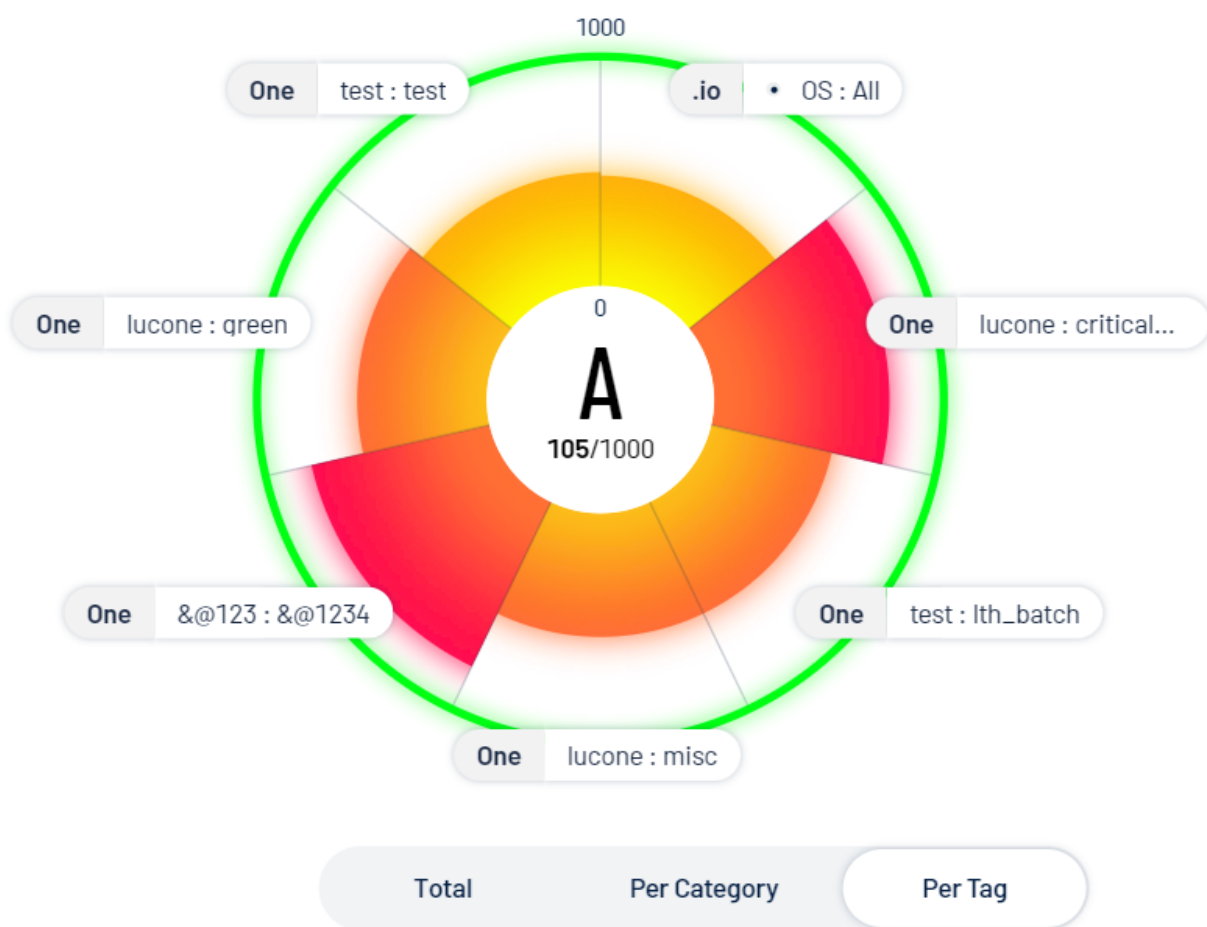
- To view the top tags driving your score, below the circle graph, click **Per Tag**.

**Note:** The **Exposure View** page displays a maximum of 10 tags within the graph.

The CES graph splits into sections that represent the top 10 tags affecting your Cyber Exposure Score. For more information, see [Tags](#).

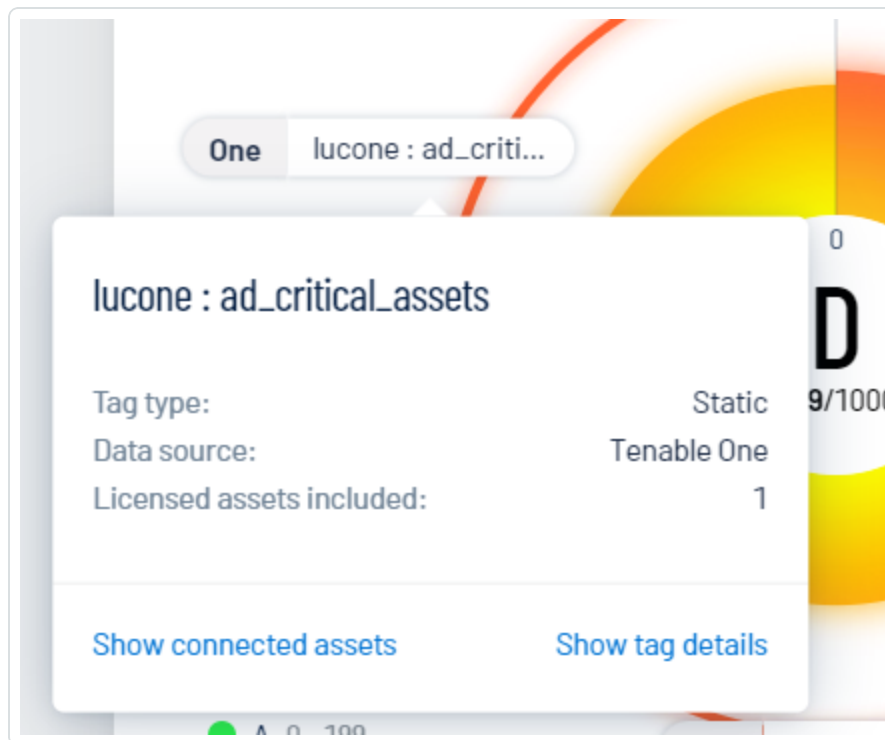


## Overall score





- Within the CES graph, click an individual tag name to view additional tag information, [connected assets](#), and [tag details](#).



- To the right of the CES graph, view a small blurb that:
  - Indicates how your score compares to the baseline target.
  - Identifies the performance of your categories. For example, this blurb may explain that you have two critical categories.
- On the right side of the page, in the **Benchmarks** section, view how your CES compares to others in your industry and in the total population.
- In the **Change** section, view how your CES has changed within the last 30 days.
- In the **Asset Risk Breakdown** section, view tiles that indicate your asset risk:
  - The **Critical Risks** tile shows the percentage of your assets with associated vulnerabilities of critical severity, as well as the data source(s) of those assets.
  - The **High Risks** tile shows the percentage of your assets with associated vulnerabilities of high severity, as well as the data source(s) of those assets.

- The **Medium/Low Risks** tile shows the percentage of your assets with associated vulnerabilities of medium or low severity, as well as the data source(s) of those assets.

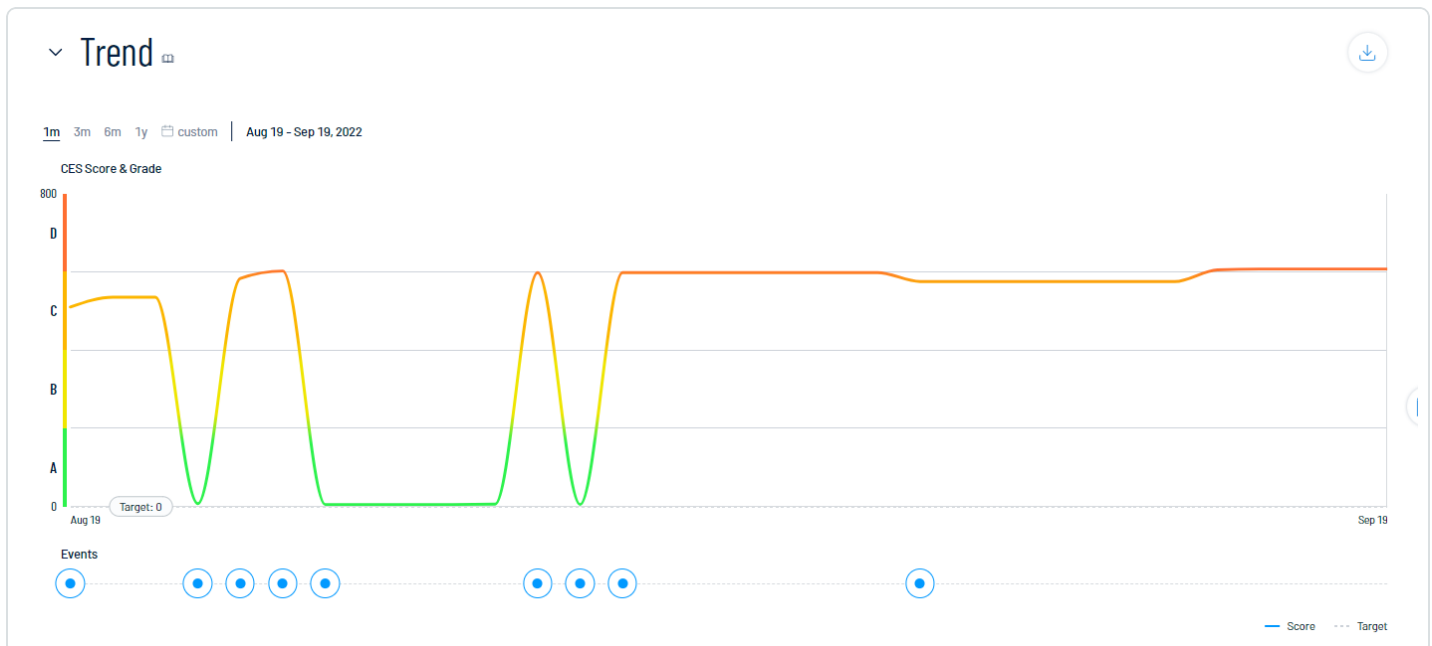
Click any tile to navigate to the [Assets](#) page filtered by the asset severity type you selected.

**Caution:** Data in the **Asset Risk Breakdown** section is based on your Vulnerability Priority Rating (VPR). As a result, if you configure your [Tenable Vulnerability Management vulnerability severity](#) setting to use CVSS, data in this section may be inconsistent.

**Note:** Since an asset can have multiple risks across all severities, the sum of the percentages in the **Asset Risk Breakdown** section may exceed 100%.

## CES Trend

The **Trend** section of the **Exposure View** page shows how your CES has trended over time. You can also view information about specific events that have contributed to your CES.



**Note:** Because exposure card scores are globally calculated, [role-based access control](#) (RBAC) does not affect card data on the **Exposure View** page.

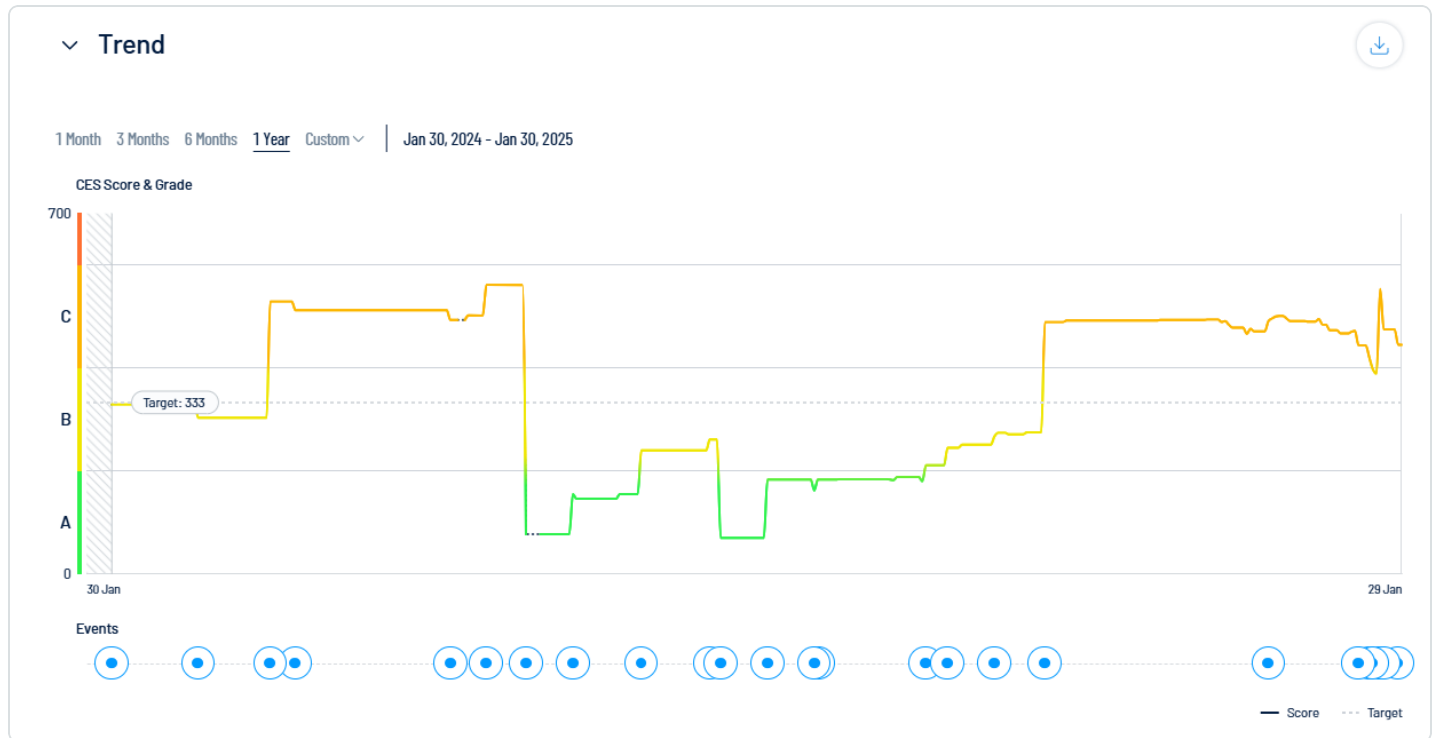
To view your CES trend for an exposure card:



1. In the [exposure card library](#), select the exposure card for which you want to view your CES trend.

The **Exposure View** page displays CES details for the selected card.

2. Scroll down to the **Trend** section.




In the **Trend** section, you can:

- View a graphical representation of your CES trend over time.
- At the top of the trend graph, select a timeframe for which you want to view your CES trend:
  - **1m** – View your CES trend over the previous month.
  - **3m** – View your CES trend over the previous 3 months.
  - **6m** – View your CES trend over the previous 6 months.
  - **1y** – View your CES trend over the previous year.
  - **Custom** date range – Use the calendar tool to select a specific date range over which to view your CES trend.





- At the bottom of the trend graph, click an  event marker. In the **Events** section, Tenable Exposure Management displays specific information about that event and how it affects your CES.

## Tag Performance

The **Tag Performance** section of the **Exposure View** page shows how the tags applied to your assets affect your CES. You can use this information to answer the following questions:

- What tags are part of my current exposure view?
- Which tags drive my CES?
- Which tags should I focus on to improve my scores?

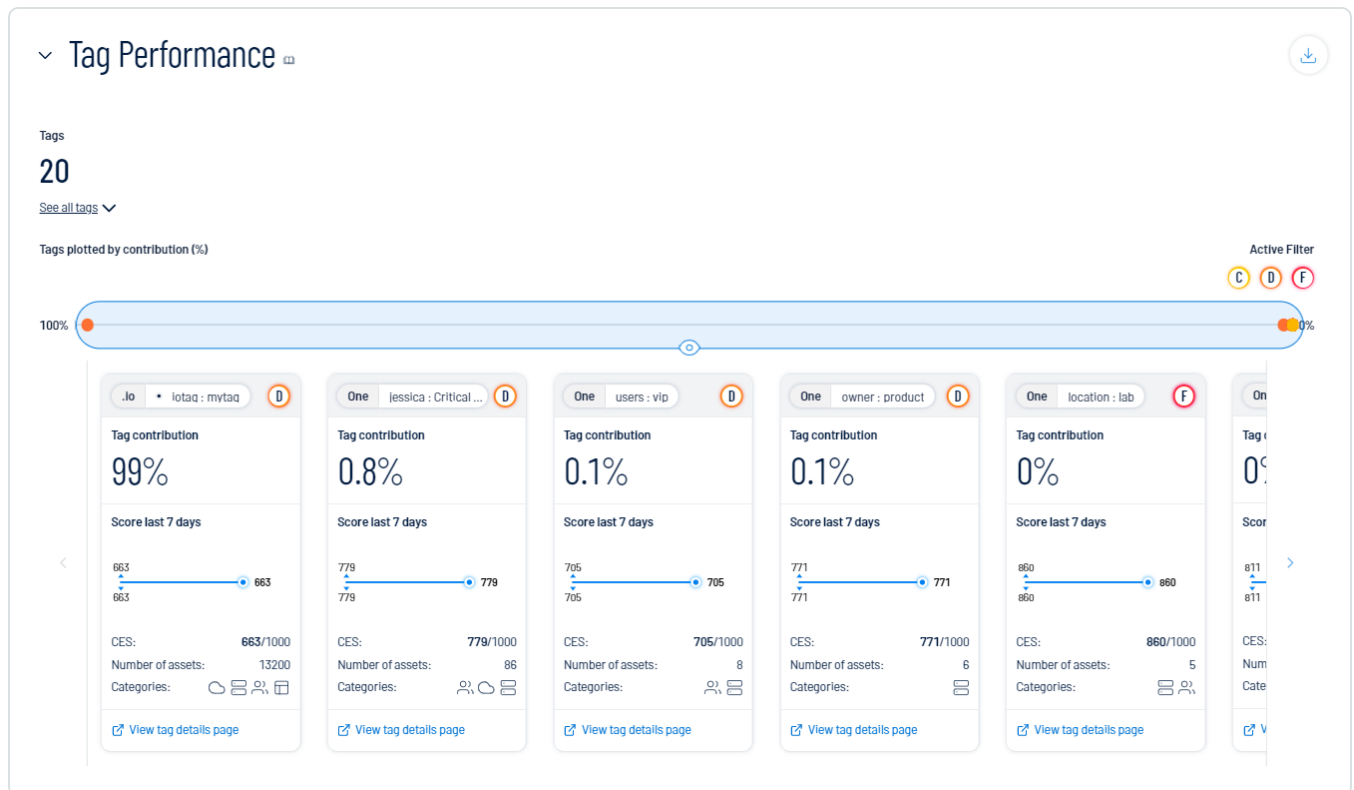
**Note:** Because exposure card scores are globally calculated, [role-based access control](#) (RBAC) does not affect card data on the **Exposure View** page.

To view your tag performance:

1. In the [exposure card library](#), select the exposure card for which you want to view your tag performance.

The **Exposure View** page displays CES details for the selected card.

2. Scroll down to the **Tag Performance** section.



In the **Tag Performance** section, you can do the following:

- View the number of tags within your Tenable Exposure Management instance.

- To see a list of all tags, click **See all tags**.

A list of your tags appears in *Category:Value* pair format.

- Click on a tag *Category:Value* pair to view additional details:

- **Tag Type** – The tag type (e.g., static).
    - **Data Source** – The application in which the tag was created. For more information, see [Data Sources](#).
    - **Show connected assets** – Click to view a list of assets to which the tag is applied. Tenable Exposure Management redirects you to the [Assets](#) page filtered by the selected tag.




- **Show tag details** – Click to view all details for the tag. Tenable Exposure Management redirects you to the [Tag Details](#) page.

- View a plot point graph of your tags based on the percentage of their contribution.

**Tip:** Click on a plot point to highlight the corresponding tile below.

**Note:** Because an asset can be tagged with more than one tag, tags can overlap, causing your total percentage to exceed 100%.

- In the **Active Filter** section, click on a letter grade score to filter all data in the **Tag Performance** section by tags that fall under the selected score.
- View tiles that highlight the performance of each tag. On any tile, you can:
  - View the name of the *Category:Value* pair.
  - View a letter grade representation of your CES grade as it compares to your industry and the total population.
  - View the **Tag contribution** percentage (i.e., the percentage of your CES score that comes from assets to which this tag is applied).
  - View a graphical representation of the CES trend over the last 7 days.
  - View the tag CES.
  - View the **Number of assets** to which the tag is applied.
  - View the **Categories** to which the tag belongs. For more information, see [Tenable Exposure Management Metrics](#).
  - Click **View tag details page** to navigate directly to the [Tag Details](#) page.
  - To the right of the tiles, click the  button to scroll through available tiles.

## Remediation SLA

The **Remediation SLA** section of the **Exposure View** page shows Remediation Service Level Agreement (SLA) data for Tenable Exposure Management. SLA represents the acceptable time frame between when a finding is discovered and when it fixed or remediated. Here, you can visualize risks by severity and by compliance with your SLAs to determine how well you are aligning



to your organization's policy.

### How is my SLA calculated?

Tenable Exposure Management calculates your SLA efficiency by comparing the number of active findings inside your SLA versus the number of active findings that are inside AND outside your SLA:

Findings inside / Findings (Inside + Outside)

Tenable Exposure Management includes all active findings in SLA calculations, but only includes remediated findings if they were fixed during the remediation timeframe. To determine if a finding is inside or outside of your SLA, compare the following finding properties:

- All active findings: *current-date / first-observed-at*
- Remediated findings: *last-fixed-at / first-observed-at*

The data in the **Remediation SLA** section applies to all exposure cards within the **Exposure View** page and are only based on vulnerability findings. Findings without a Vulnerability Priority Rating (VPR) do not count towards SLA calculations.

**Tip:** You can edit your SLA in Tenable Exposure Management by configuring your [Exposure View page settings](#).

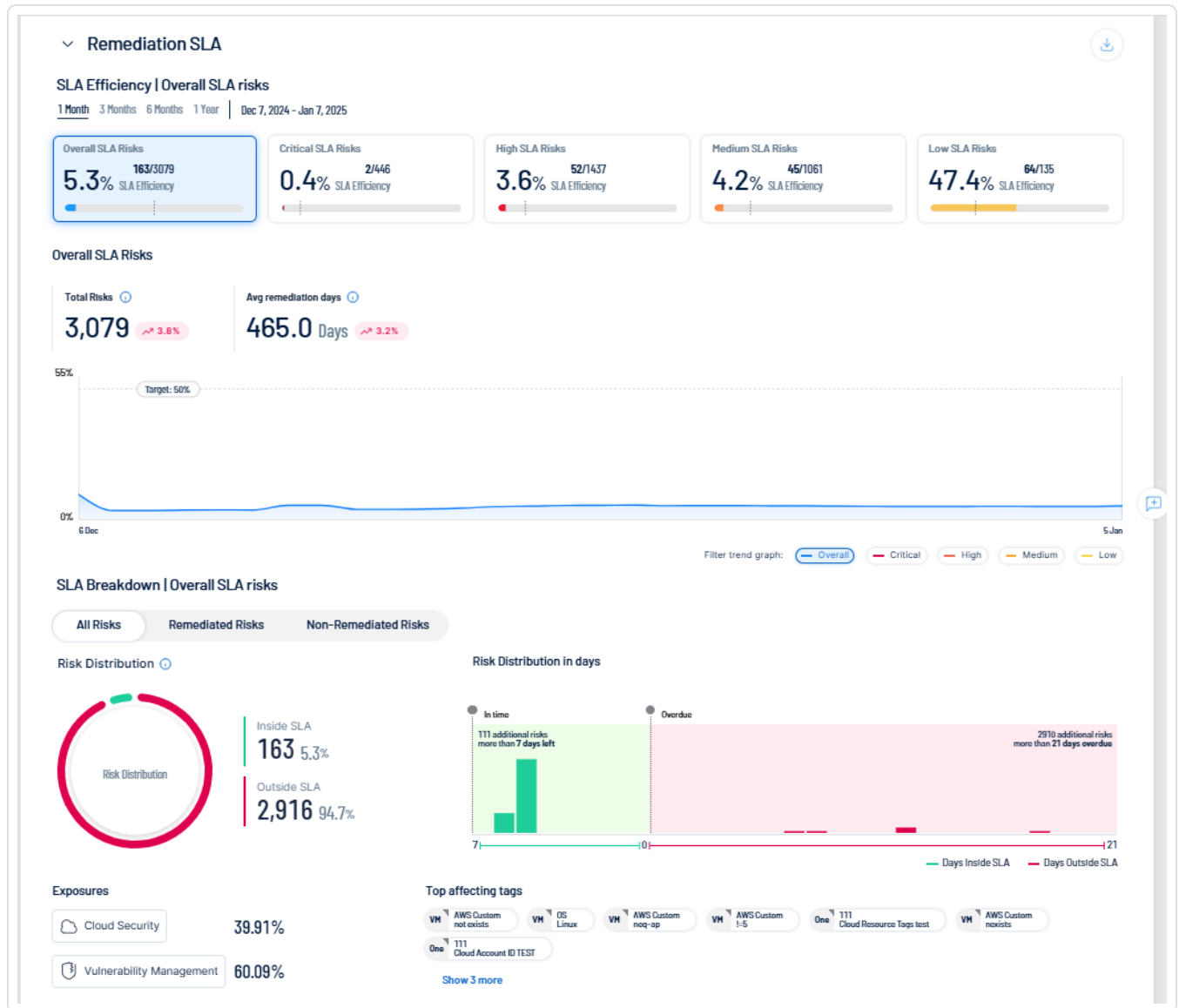
**Note:** Because exposure card scores are globally calculated, [role-based access control](#) (RBAC) does not affect card data on the **Exposure View** page.

To view remediation SLA data:

1. In the [exposure card library](#), select the exposure card for which you want to view your tag performance.

The **Exposure View** page displays CES details for the selected card.

2. Scroll down to the **Remediation SLA** section.



In the **Remediation SLA** section, you can:

- Select a timeframe for which you want to view the Remediation SLA data:
  - **1 Month** —View Remediation SLA data for the previous month.
  - **3 Months** —View Remediation SLA data for the previous 3 months.
  - **6 Months** —View Remediation SLA data for the previous 6 months.
  - **1 Year** —View Remediation SLA data for the previous year.

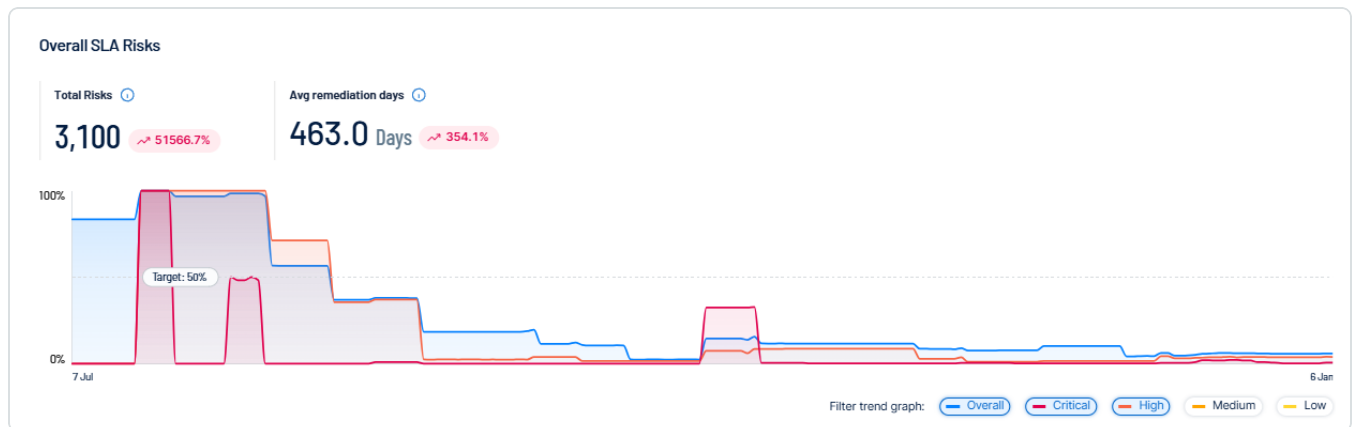


All data within the **Remediation SLA** section updates accordingly, including the **SLA Efficiency** and **SLA Breakdown** subsections.

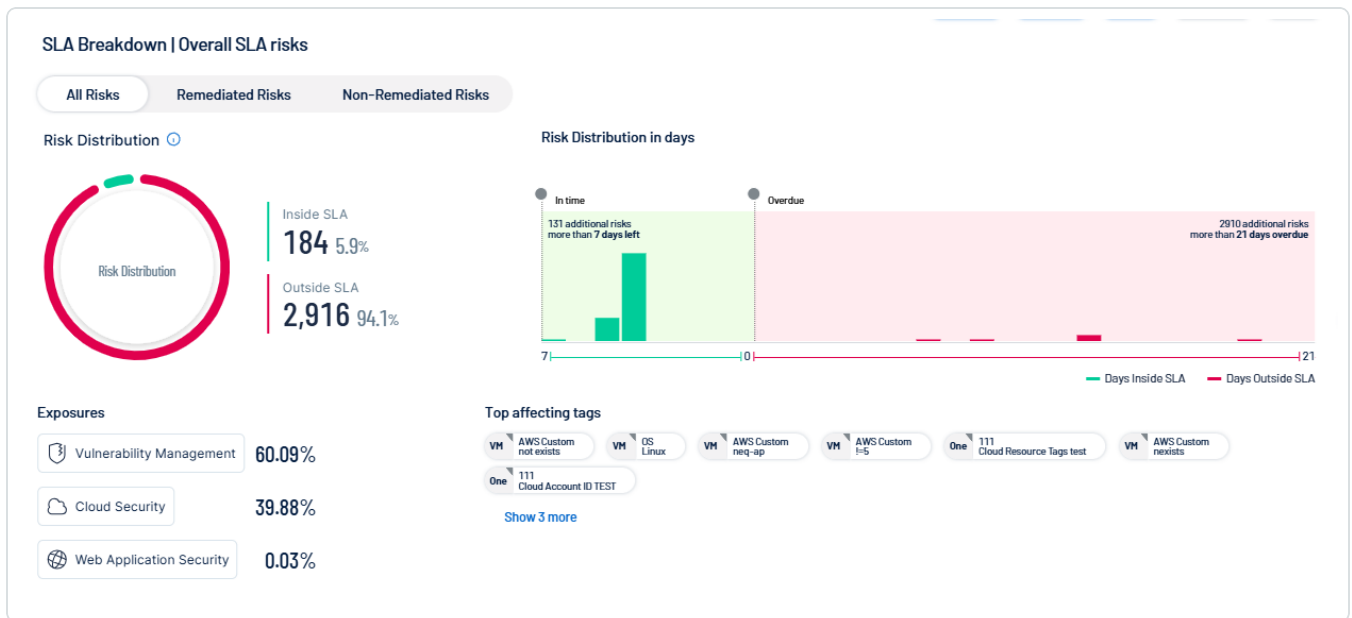
- Select a severity level by which you want to filter Remediation SLA data:
  - **Overall SLA Risks** – View risks for your overall SLA.
  - **Critical SLA Risks** – View only risks that have a critical severity.
  - **High SLA Risks** – View only risks that have a high severity.
  - **Medium SLA Risks** – View only risks that have a medium severity.
  - **Low SLA Risks** – View only risks that have a low severity.

All data within the **Remediation SLA** section updates accordingly, including the **SLA Efficiency** and **SLA Breakdown** subsections.

- In the trend graph, view SLA trend metrics for the selected range of dates.



- At the bottom of the trend graph, click one or more severity filters to view on the graph. Multiple severities overlap on the graph to show a holistic view of your SLA risk over time.
- View your **SLA Breakdown**:



- Click a risk group type to filter the **SLA Breakdown** data:
  - **All Risks** – All risks regardless of remediation status.
  - **Remediated Risks** – Only remediated risks.
  - **Non-remediated Risks** – Only non-remediated risks.
- View a graphical representation of your **Risk distribution**, which shows the number and percentage of risks that fall **Inside SLA** and **Outside SLA**.
- View a graphical representation of your **Risk distribution in days**, which shows your risk distribution based on the number of days your risks are inside or outside the SLA.
- View the percentage of **Exposures** that come from specific exposure categories, for example, **Cloud Security**. For more information, see [Exposure Categories](#).
- In the **Top Affecting Tags** section, view the top tags outside of your SLA, listed in descending order. Click on a tag to view additional details.

Additionally, you can manage the **Exposure View** page in the following ways:

- [Comment](#) on the **Exposure View** page.
- [Export](#) the **Exposure View** page.
- [Configure](#) the **Exposure View** page settings.

## Manage the Exposure View Page





In Tenable Exposure Management, you can manage and interact with the [Exposure View](#) page in the following ways:

### Comment on the Exposure View Page

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

You can comment on any section within the **Exposure View** page. Depending on their permissions and notification settings, users within your Tenable Exposure Management instance can view your comments. For more information, see [View Comment Notifications](#).

To comment on the **Exposure View** page:

1. Access the [Exposure View](#) page.
2. Do one of the following:
  - In the upper-right corner of the view, click the  button.
  - Scroll to the section on which you want to comment and click the  button.

The **Comments** pane appears.





Comments

×

Tue Jun 21 2022

MA

You

Today at 11:54 AM

Cyber Exposure Score

Looks great!

Commenting on Cyber Exposure Score

Leave a comment or add others by using @


↑

☐

Include snapshot



**Tip:** If you scroll up or down within the **Exposure View** page, the **Comments** pane automatically adjusts to add the comment to the currently displayed section.

3. In the text box, type your comment.
4. (Optional) To include a snapshot of the section on which you want to comment, select the **Include snapshot** check box.
5. Click the  button.


Tenable Exposure Management posts your reply. Depending on their permissions and notification settings, Tenable Exposure Management notifies other users about your comment.

### View Comment Notifications

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

When someone comments on the **Exposure View** page, a notification appears in the **Comments** window. For more information about commenting on the **Exposure View** page, see [Comment on the Exposure View Page](#).

To view comment notifications:


1. Access the [Exposure View](#) page.
2. In the upper-right corner, click the  button.

The **Comments** window appears and shows your unseen comments and replies.

3. (Optional) To reply to a comment, click on the comment.

The **Comments** pane appears and displays the selected comment.

- a. In the text box, type your comment.
- b. (Optional) To include a snapshot of the section on which you want to comment, select the **Include snapshot** check box.

- 
- c. Click the  button.

Tenable Exposure Management posts your reply. Depending on their permissions and notification settings, Tenable Exposure Management notifies other users about your comment.

### Export a Section or All of the Exposure View Page

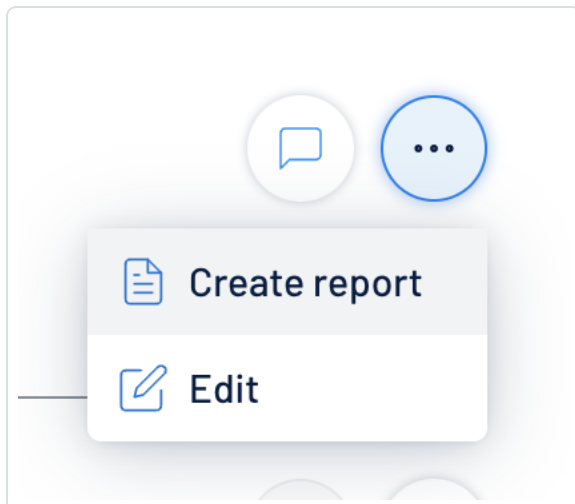
You can export **Exposure View** page data in the following ways:

- Export the entire **Exposure View** page in .pdf format
- Export a single section of the **Exposure View** page in .png format.

To export the entire **Exposure View** page:

1. Access the [Exposure View](#) page.
2. In the upper right corner, click the  button.

A menu appears.




3. Click  **Create Report**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

To export a single section of the **Exposure View** page:




1. Access the [Exposure View](#) page.
2. Scroll to the section of the page that you want to export.
3. Click the  button.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

### Configure Exposure View Page Settings

You can configure how data appears within on the [Exposure View](#) page, including system defaults and benchmarks, layouts, and data sorting.

To configure your **Exposure View** page settings:

1. Access the [Exposure View](#) page.
2. In the upper-right corner, click the  button.

The **Exposure View Settings** page appears.



# Lumin Exposure View Settings

## Exposure Card Library

### Sparkline Timespan

1 week

### Card sorting

- ☐ Manual Sort
- ☐ Alphabetic Order
- ☒ Creation Order
- ☐ Last Modified Order
- ☐ Score (Low To High CES)
- ☐ Score (High To Low CES)

## Exposure Card Defaults

### Benchmark Industry

Media

### Card Layout

Show Metric	Name	Open by default	Drag to reorder
<input checked="" type="checkbox"/>	SLA	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Feed	<input checked="" type="checkbox"/>	

- (Optional) Configure settings in the following sections:



- **Exposure Card Library**

Option	Description
<b>Sparkline Timespan</b>	In the drop-down menu, select the timespan to use for the sparkline preview on exposure cards within the <b>Exposure Cards</b> library.
<b>Card sorting</b>	Select the radio button for how you want to sort the cards within the <b>Exposure Cards</b> library.

- **Exposure Card Defaults**

Option	Description
<b>Benchmark Industry</b>	In the drop-down menu, select the industry to use as a benchmark when comparing your metrics. For more information, see <a href="#">Tenable Exposure Management Metrics</a> .
<b>Show Metric</b>	Do any of the following: <ul style="list-style-type: none"><li>◦ Select the check box next to any metric that you want to include on the <b>Exposure View</b> page.</li><li>◦ Deselect the check box next to any metric that you do not want to include on the <b>Exposure View</b> page.</li></ul>
<b>Name</b>	View the name of the metric for which you're configuring the card layout.
<b>Open by default</b>	Do any of the following: <ul style="list-style-type: none"><li>◦ Enable the toggle for any metric that you want to open by default when viewing the <b>Exposure View</b> page.</li><li>◦ Disable the toggle for any metric that you do not want to open by default when viewing the <b>Exposure View</b> page.</li></ul>



<b>Drag to reorder</b>	Drag and drop the rows of metrics to edit the order in which they appear within the <b>Exposure View</b> page.
<b>Card Targets</b>	<p>The <b>Card Targets</b> section allows you set the overall target for the card.</p> <p>Select the radio button next to one of the following options:</p> <ul style="list-style-type: none"><li>◦ <b>Custom</b> — Manually select a target benchmark for the exposure card by doing one of the following:<ul style="list-style-type: none"><li>■ In the text box, manually type a target benchmark number for the card.</li><li>■ Click and drag the slider to select a target benchmark number for the card.</li></ul></li><li>◦ <b>Set to Industry Benchmark</b> — Automatically set the target to match the industry benchmark for the data.</li><li>◦ <b>Set to Population Benchmark</b> — Automatically set the target to match the population benchmark for the data.</li></ul>
<b>Category Targets</b> <ul style="list-style-type: none"><li>◦ <b>Computing Resources</b></li><li>◦ <b>Cloud Resources</b></li><li>◦ <b>Identities</b></li><li>◦ <b>Web Applications</b></li></ul>	<p>The <b>Category Targets</b> section allows you set the target benchmark for each individual category whose data populates the <b>Exposure View</b> page.</p> <div><b>Note:</b> These settings only apply to the <a href="#">Score</a> toggle view of the <b>Exposure View</b> page.</div> <p>For each category, select the radio button next to one of the following options:</p> <ul style="list-style-type: none"><li>◦ <b>Custom</b> — Manually select a target benchmark for</li></ul>



<ul style="list-style-type: none"><li>◦ <b>Operational Technology</b></li></ul>	<p>the category by doing one of the following:</p> <ul style="list-style-type: none"><li>■ In the text box, manually type a target for the category.</li><li>■ Click and drag the slider to select a target for the category.</li></ul> <ul style="list-style-type: none"><li>◦ <b>Set to Industry Benchmark</b> – Automatically set the target to match the industry benchmark for the data.</li><li>◦ <b>Set to Population Benchmark</b> – Automatically set the target to match the population benchmark for the data.</li></ul>
<b>Exposure Card Targets</b>	<p>The <b>Exposure Card Targets</b> section allows you set the target benchmark for exposure cards within the <b>Exposure View</b> page.</p> <p>For each category, select the radio button next to one of the following options:</p> <ul style="list-style-type: none"><li>◦ <b>Custom</b> – Manually select a target benchmark for the category by doing one of the following:<ul style="list-style-type: none"><li>■ In the text box, manually type a target for the category.</li><li>■ Click and drag the slider to select a target for the category.</li></ul></li><li>◦ <b>Set to Industry Benchmark</b> – Automatically set the target to match the industry benchmark for the data.</li><li>◦ <b>Set to Population Benchmark</b> – Automatically set the target to match the population benchmark for</li></ul>





	the data.
<b>Exposure Targets</b> <ul style="list-style-type: none"><li>◦ <b>Cloud Security</b></li><li>◦ <b>Identity Exposure</b></li><li>◦ <b>OT Security</b></li><li>◦ <b>Vulnerability Management</b></li><li>◦ <b>Web Application Security</b></li></ul>	<p>The <b>Exposure Targets</b> section allows you set the target benchmark for each individual Exposure Management Class whose data populates Tenable Exposure Management.</p> <p>For each category, select the radio button next to one of the following options:</p> <ul style="list-style-type: none"><li>◦ <b>Custom</b> – Manually select a target benchmark for the category by doing one of the following:<ul style="list-style-type: none"><li>■ In the text box, manually type a target for the category.</li><li>■ Click and drag the slider to select a target for the category.</li></ul></li><li>◦ <b>Set to Industry Benchmark</b> – Automatically set the target to match the industry benchmark for the data.</li><li>◦ <b>Set to Population Benchmark</b> – Automatically set the target to match the population benchmark for the data.</li></ul>

- **Trend**

Option	Description
<b>Default Timespan Shown</b>	In the drop-down menu, select the timespan to use for the <a href="#">CES Trend</a> section within the <b>Exposure View</b> page.

- **Remediation SLA**



Option	Description
<b>Risk Severity</b>	Do any of the following: <ul style="list-style-type: none"><li>◦ Select the check box next to any risk severity you want to include within the <a href="#">Remediation SLA</a> section on the <b>Exposure View</b> page.</li><li>◦ Deselect the check box next to any risk severity you want to include within the <a href="#">Remediation SLA</a> section on the <b>Exposure View</b> page.</li></ul>
<b>Data Categories /Remediation (in days)</b>	For each data category, type the number of days within which each risk level of SLA must be addressed. For example, if you have an internal SLA to address critical <b>Computing Resources</b> risks within 4 days, in the <b>Critical</b> text box for that category, type <b>4</b> .
<b>SLA Efficiency Target</b>	For each risk severity, drag the slider to set the SLA efficiency target percentage to use within the <b>Exposure View</b> page.
<b>Graph Range</b>	For each risk range, type the date range to use for the graph in the <b>SLA</b> section within the <b>Exposure View</b> page.

4. Click **Save** .

Tenable Exposure Management saves your configuration updates and applies any changes.

## Manage Exposure Cards

In Tenable Exposure Management, you can manage exposure cards in the following ways:

### Create a Custom Exposure Card

In Tenable Exposure Management, you can create a custom exposure card to specify the categories for which you want to see data. Once you create a custom exposure card, you can then select the card in the [exposure card library](#) to view its data on the **Exposure View** page.

Before you begin:

- (Optional) [Create a tag](#) to apply to the card.

To create a custom exposure card:

1. At the top of the [exposure card library](#), click the **+ New Custom Card** button.

The **New Custom Card** page appears.

## New Custom Card

### Card Details

**\* Card Name**

**\* Card Description**

Enter a card description

### Adding Tags

Search tags

Tag Name	CES	Related Assets	Weaknesses
<input type="checkbox"/> <b>VM</b> AWS Custom neq-ap	<div><div></div></div> 492	7,124	<div><div></div></div> 6.8k
<input type="checkbox"/> <b>VM</b> AWS Custom nexists	<div><div></div></div> 492	7,124	<div><div></div></div> 6.8k
<input type="checkbox"/> <b>VM</b> AWS Custom l-e	<div><div></div></div> 492	7,124	<div><div></div></div> 6.8k
<input type="checkbox"/> <b>VM</b> AWS Custom not exists	<div><div></div></div> 492	7,021	<div><div></div></div> 6.8k

2. In the **Card Details** section:
  - a. In the **Card Name** box, type a name for the exposure card.
  - b. In the **Card Description** box, type a brief description of the exposure card.
3. In the **Adding Tags** section, select the tags you want to use to provide data for the exposure card:



- a. (Optional) Use the **Search** box to search for specific tags.
- b. Select the check box next to each tag you want to use to provide data for the exposure card.

4. Click **Save**  .

Tenable Exposure Management saves the exposure card and adds it to the **Custom** tab within the [exposure card library](#).

**Tip:** You can later edit the card to configure more settings such as the card layout and targets, as well as change the defaults for card's **Trend** and **Remediation SLA**.

## Edit an Exposure Card

To edit an exposure card:

1. In the [exposure card library](#), click the card you want to edit.

The card information appears.

2. In the upper right corner of the page, click the  button.

A menu appears.

3. Click  **Edit**.

The edit card page appears.



Card Settings

Card Name

Cloud Security

Max. 60 characters14/60

Card Description

Cloud Resources

Benchmark Industry

Other

Card Layout

Show Metric	Name	Open by default	Drag to reorder
<input checked="" type="checkbox"/>	Trend	<input checked="" type="checkbox"/>	<div></div>
<input checked="" type="checkbox"/>	SLA	<input checked="" type="checkbox"/>	<div></div>
<input checked="" type="checkbox"/>	Tag Performance	<input checked="" type="checkbox"/>	<div></div>

Exposure card targets

F

1000

Default☒ Custom

4. On the **Card Settings** tab, make any desired changes:

- **Card Settings**

Option	Description
Card Name	Edit the name of the card.
Card Description	Edit the card description.

- **Benchmark Industry**

Option	Description
--------	-------------



<b>Benchmark Industry</b>	In the drop-down menu, select the industry to use as a benchmark when comparing your metrics. For more information, see <a href="#">Tenable Exposure Management Metrics</a> .
---------------------------	---

- **Card Layout**

Option	Description
<b>Show Metric</b>	Do any of the following: <ul style="list-style-type: none"><li>• Select the check box next to any metric that you want to include in the exposure card.</li><li>• Deselect the check box next to any metric that you do not want to include in the exposure card.</li></ul>
<b>Open by Default</b>	Do any of the following: <ul style="list-style-type: none"><li>• Enable the toggle for any metric that you want to open by default when viewing the exposure card.</li><li>• Disable the toggle for any metric that you do not want to open by default when viewing the exposure card.</li></ul>
<b>Drag to Reorder</b>	Drag and drop the rows of metrics to edit the order in which they appear on the exposure card.

- **Exposure Card Targets**

Option	Description
<b>Default/Custom toggle</b>	Do any of the following: <ul style="list-style-type: none"><li>• Enable the toggle to use the default options for this section.</li><li>• Disable the toggle to set custom options for this section.</li></ul>



### Card Targets

The **Card Targets** section allows you set the overall target for the card.

Select the radio button next to one of the following options:

- **Custom** – Manually select a target benchmark for the exposure card by doing one of the following:
  - In the text box, manually type a target benchmark number for the card.
  - Click and drag the slider to select a target benchmark number for the card.
- **Set to Global Target** – Automatically set the target to match your Global CES for the data.
- **Set to Industry Benchmark** – Automatically set the target to match the industry benchmark for the data.
- **Set to Population Benchmark** – Automatically set the target to match the population benchmark for the data.

- **Exposure Targets** (Custom Cards Only)

Option	Description
<b>Exposure Targets</b> <ul style="list-style-type: none"><li>• <b>Vulnerability Management</b></li><li>• <b>Web Applications</b></li><li>• <b>Identity Exposure</b></li></ul>	<p>The <b>Exposure Targets</b> section allows you set the target benchmark for each individual category whose data populates the card.</p> <p>For each category, select the radio button next to one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Custom</b> – Manually select a target benchmark for the category by doing one of the following:<ul style="list-style-type: none"><li>◦ In the text box, manually type a target for the</li></ul></li></ul>



<ul style="list-style-type: none"><li>• <b>Operational Technologies</b></li><li>• <b>Cloud Security</b></li></ul>	<p>category.</p> <ul style="list-style-type: none"><li>◦ Click and drag the slider to select a target for the category.</li></ul> <ul style="list-style-type: none"><li>• <b>Set to Global Target</b> – Automatically set the target to match your Global CES for the data.</li><li>• <b>Set to Industry Benchmark</b> – Automatically set the target to match the industry benchmark for the data.</li><li>• <b>Set to Population Benchmark</b> – Automatically set the target to match the population benchmark for the data.</li></ul>
---	---

- **Trend**

Option	Description
<b>Default/Custom</b> toggle	Do any of the following: <ul style="list-style-type: none"><li>• Enable the toggle to use the default options for this section.</li><li>• Disable the toggle to set custom options for this section.</li></ul>
<b>Default Timespan Shown</b>	In the drop-down menu, select the timespan to use for the <b>Trend</b> section within Tenable Exposure Management.

- **Remediation SLA**

Option	Description
<b>Default/Custom</b> toggle	Do any of the following: <ul style="list-style-type: none"><li>• Enable the toggle to use the default options for this section.</li></ul>





	<ul style="list-style-type: none"><li>• Disable the toggle to set custom options for this section.</li></ul>
<b>Low, Medium, High, and Critical</b> ranges	For each category, type the number of days within which each risk level of SLA must be addressed. For example, if you have an internal SLA to address critical <b>Computing Resources</b> risks within 4 days, in the <b>Critical</b> text box for that category, type <b>4</b> .
<b>View Severity on Card</b>	Do any of the following: <ul style="list-style-type: none"><li>• Select the check box below any risk range that you want to include in the exposure card.</li><li>• Deselect the check box below any risk range that you do not want to include in the exposure card.</li></ul>
<b>Graph Range</b>	For each risk range, type the date range to use for the graph in the <b>SLA</b> section within Tenable Exposure Management.

5. Click **Save** .

Tenable Exposure Management saves your changes to the exposure card.

## Share a Custom Exposure Card

**Note:** You can only share custom exposure cards.

To share a custom exposure card:

1. In the [exposure card library](#), click the **Custom** tab.

A list of user-created custom cards appears.

2. Click the custom card you want to share.

The card information appears.

3. At the top of the page, click **Share** .

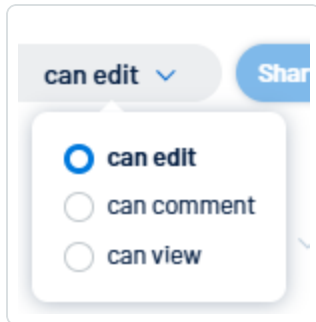
The **Share Exposure Card** window appears.



4. In the search box, type the email address of the user or users with which you want to share the exposure card data.

**Tip:** Below the search box, you can view which users have access to the data.

5. In the drop-down menu, select the access you want to grant to the user with which you are sharing the exposure card data. For example, if you want to allow the user to comment on the data, select **can comment**.



6. Click **Share**.

Tenable Exposure Management shares the exposure card data with the selected users. Selected users receive notification emails.

## Delete a Custom Exposure Card

**Note:** You can only delete custom exposure cards.

To delete a custom exposure card:

1. In the [exposure card library](#), click the **Custom** tab.

A list of user-created custom cards appears.

2. Click the custom card you want to delete.

The card information appears.

3. At the top of the page, click the  button.

A menu appears.

4. Click  **Edit**.



The edit card page appears.

Card Settings

\* Card Name

Cloud Security

Max. 60 characters14/60

Card Description

Cloud Resources

Benchmark Industry

Other

Card Layout

Show Metric	Name	Open by default	Drag to reorder
<input checked="" type="checkbox"/>	Trend	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	SLA	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Tag Performance	<input checked="" type="checkbox"/>	

Exposure card targets


F







1000

☒ Custom

Default ☒ Custom

5. At the bottom of the page, click **Delete**



Risk Severity	<input checked="" type="checkbox"/> Overall Risks	<input type="checkbox"/> Critical Risks	<input checked="" type="checkbox"/> High Risks	<input checked="" type="checkbox"/> Medium Risks	<input checked="" type="checkbox"/> Low Risks
Data Categories	Remediation (in days)				
 <b>Computing Resources</b> -	<input type="text" value="3"/> Days	<input type="text" value="3"/> Days	<input type="text" value="3"/> Days	<input type="text" value="3"/> Days	<input type="text" value="3"/> Days
SLA Efficiency Target	<input type="text" value="50%"/> 	<input type="text" value="50%"/> 	<input type="text" value="61%"/> 	<input type="text" value="50%"/> 	<input type="text" value="50%"/> 
SLA Breakdown - Graph Range					
<b>Inside SLA</b>	<input type="text" value="7"/> Days	<input type="text" value="7"/> Days	<input type="text" value="6"/> Days	<input type="text" value="7"/> Days	<input type="text" value="7"/> Days
<b>Outside SLA</b>	<input type="text" value="-21"/> Days	<input type="text" value="-21"/> Days	<input type="text" value="-52"/> Days	<input type="text" value="-21"/> Days	<input type="text" value="-21"/> Days

A confirmation message appears.

6. Click **Delete card**.

Tenable Exposure Management deletes the custom exposure card.



## Attack Path

As part of a typical attack, adversaries leverage different tools and techniques to accomplish their objectives. Usually, a hacker attains an initial foothold over the network, whether by a phishing attack or exploiting a publicly exposed vulnerability. Hackers may then seem to maintain access over the machine (Persistence), elevate their privileges, and laterally pivot between network devices (Lateral Movement). Last, the hacker tries to complete their objective, for example, a denial of service of critical infrastructure, exfiltration of sensitive information, or distraction of existing services. This event is known as *Attack Path*. An attack path contains one or more *Attack Techniques*, allowing the hacker to accomplish his objective.

The **Attack Path** page in Tenable Exposure Management takes your data and pairs it with advanced graph analytics and the MITRE ATT&CK™ Framework to create [Top Attack Techniques](#). These paths allow you to understand and take action on the unknowns that enable and amplify threat impact on your assets and information.

Additionally, you can use the [Top Attack Paths](#) tab to dive deeper into the mind of an attacker by interacting directly with attack paths, building custom paths, and manipulating the origins and targets within a path to view exactly how these changes affect your data.

**Note:** Attack path data ingestion can take up to 5 hours.

### What is Attack Path?

- *What is a top attack path?*
  - A top attack path is an attack path that leads to one or more critical assets.
- *What is a top attack technique?*
  - A top attack technique is an attack technique that exists in one or more attack paths that lead to one or more critical assets.
- *How does Tenable Exposure Management map critical assets?*



- Assets with an Asset Criticality Rating of 7 and above
- Cloud resource assets marked as Sensitive
- User account assets within Active Directory with Domain Admin rights
- *How does Tenable Exposure Management classify the severity of an attack technique?*
  - Likelihood: The number of attack paths
  - Impact: The critical assets that could be compromised by the attack
  - Method: The tactic associated with the attack (for example, lateral movement or privilege escalation)
  - Path: The start and end points of the attack path technique

Before you begin:

For Attack Path data ingestion to function as expected, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
  - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** [scan template](#). This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

**Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

- [Tenable Identity Exposure](#) SaaS deployed.

**Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Tenable Exposure Management. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:



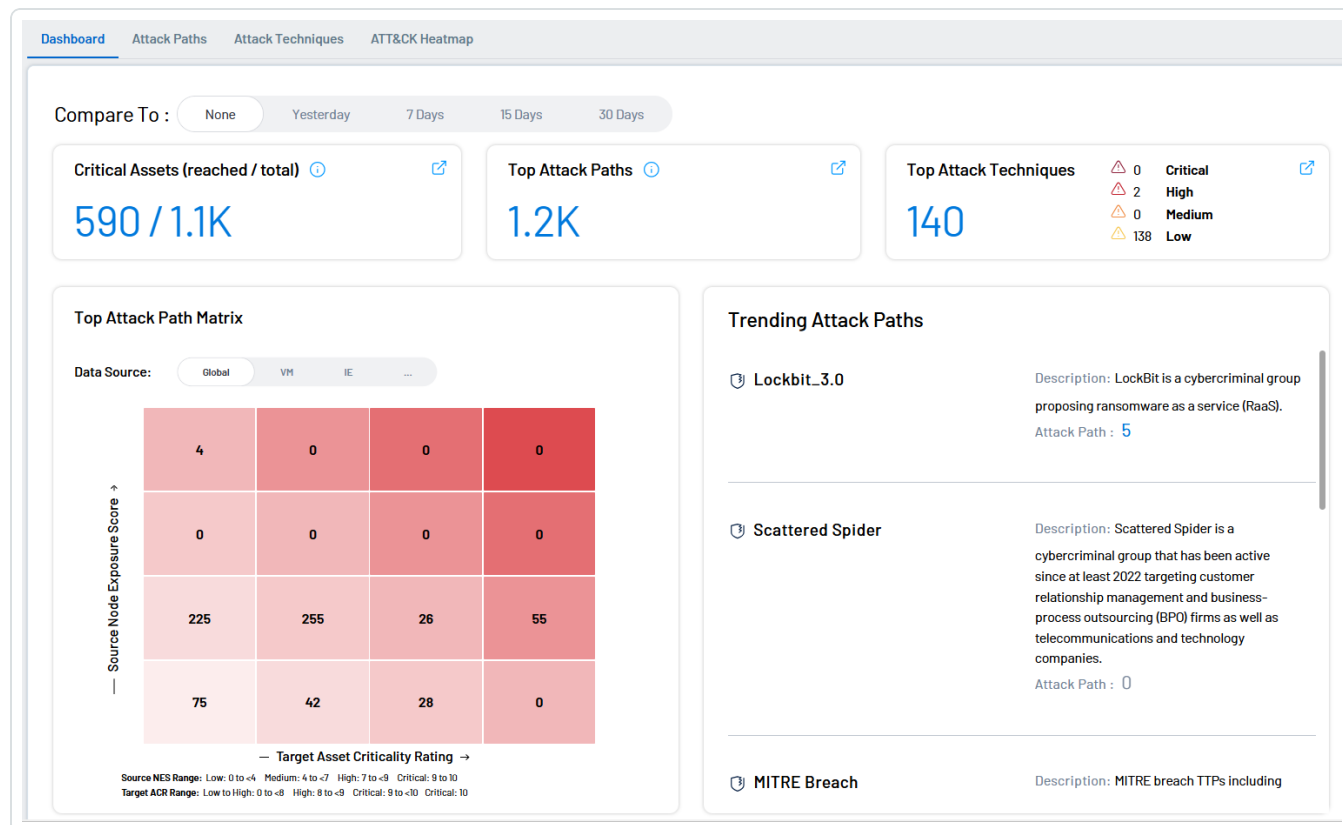
- Have at least 40% of assets scanned via an authenticated scan.
- Select maximum verbosity in the Basic Network Scan.
- A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.
- An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
- When using Tenable Identity Exposure, enable [privileged analysis](#). This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
- A scan frequency of at least once a week.
- Configure Tenable OT Security.
- Configure Tenable Attack Surface Management and [configure the application for use with Tenable Vulnerability Management](#). This ensures that usable data gets pulled into Tenable Exposure Management.

To access the **Attack Path** page:



1. In the left navigation menu, click **Attack Path**.

The **Attack Path** page appears with the **Dashboard** tab displayed by default.



On the **Attack Path** page, you can:

- View and interact with the data on the [Dashboard](#) tab.
- View and interact with the data on the [Attack Paths](#) tab.
- View and interact with the data on the [Attack Techniques](#) tab.
- View and interact with the data on the [ATT&CK Heatmap](#) tab.

## Dashboard

The **Dashboard** tab gives you a high-level view of your vulnerable assets such as the number of vulnerable critical assets, the number of attack paths leading to these critical assets, the number of open attack techniques and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.

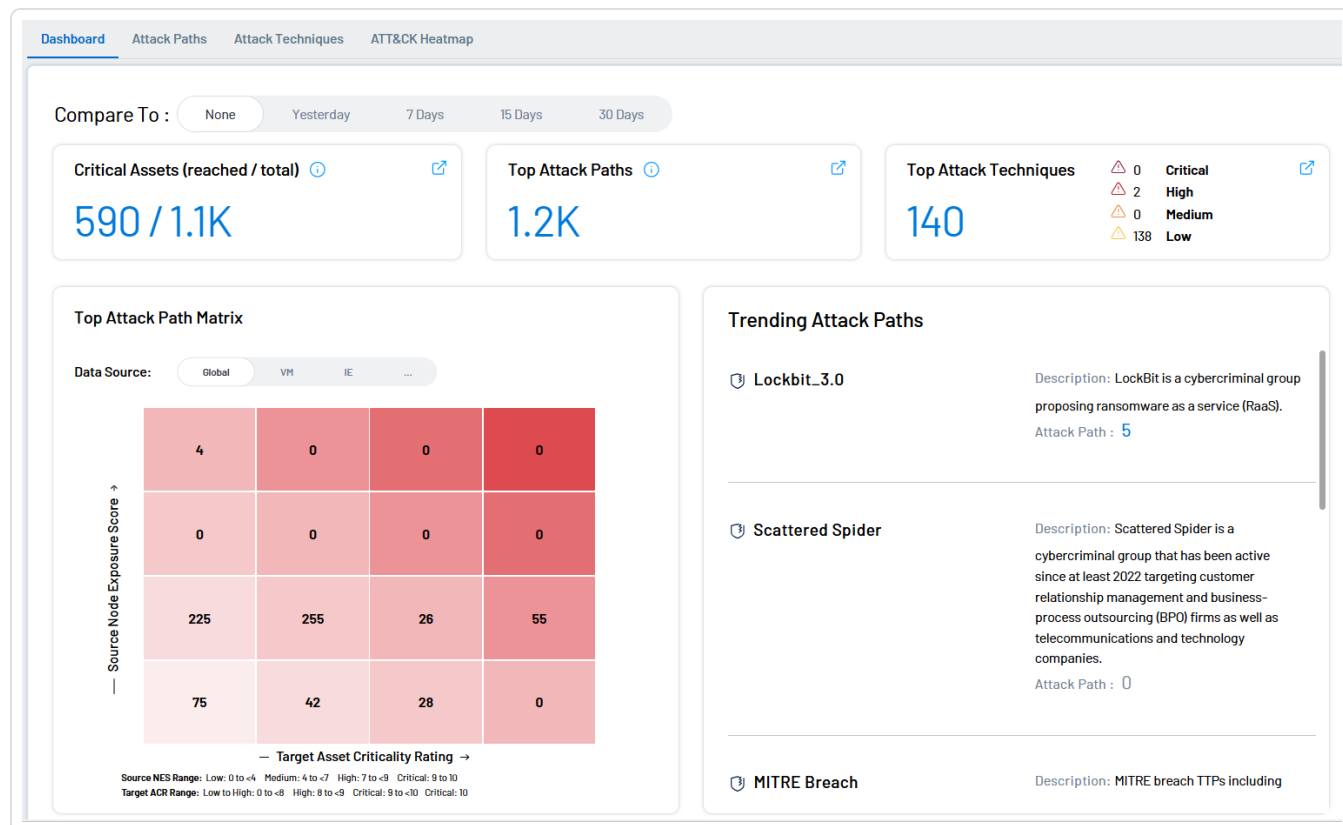
To access the **Dashboard** tab:





1. Access the [Attack Path](#) page.




The **Dashboard** tab appears by default.



The **Dashboard** tab shows the following details:

Widget	Description
Compare To	<p>Compare and view the difference between the current data and the data from a specific timeframe. You can select from these options:</p> <ul style="list-style-type: none"><li>• <b>None</b></li><li>• <b>Yesterday</b></li><li>• <b>7 days</b></li><li>• <b>15 days</b></li><li>• <b>30 days</b></li></ul> <p>Based on the option you select, each widget lists the differences between timeframes and shows a colored directional arrow to indicate</p>



	whether the value has increased or decreased.
<b>Critical Assets (reached/total)</b>	The number of critical assets that attack paths can lead to by the total number of critical assets in your environment. Click the  icon to view the reached critical assets on the <a href="#">Top Attack Paths</a> tab.
<b>Top Attack Paths</b>	The number of top attack paths that lead to critical assets. Click the  icon to view the attack paths on the <a href="#">Top Attack Paths</a> tab.
<b>Top Attack Techniques</b>	The total number of top attack techniques with the number of critical, high, medium, and low severity attack techniques. Click  to view the techniques on the <a href="#">Top Attack Techniques</a> tab.
<b>Top Attack Path Matrix</b>	<p>Each square in the matrix shows the number of attack paths corresponding to target Asset Criticality Rating (ACR) and Source Node Exposure Score values. This matrix includes only assets with an ACR of 7 or higher to ensure you can prioritize your most critical assets first.</p> <p>For example, you can quickly view the attack paths that lead to the highest ACR targets and whose source nodes have the highest exposure score source by checking the value in the square in the upper right corner of the matrix. Click any square to navigate to the <a href="#">Top Attack Paths</a> tab with the appropriate filter automatically applied. Here you can view paths that match the selected value.</p> <div><b>Tip:</b> At the top of the matrix, click on a <b>Data Source</b> to filter the matrix by attack paths from the selected source. If there is no data available for a data source type, the button for that source is disabled.</div>
<b>Trending Attack Paths</b>	A list of all trending attack paths.

## Top Attack Paths

The **Top Attack Paths** tab on the **Attack Path** page allows you to dive deeper into the mind of an attacker by interacting directly with attack paths and nodes. Here, you can:



- Use the [Attack Path Query Builder](#) to generate custom paths and manipulate the origins and targets within a path to view exactly how these changes affect your data.
- Use the [Asset Query Builder](#) to gain insight into your asset nodes and how they connect to one another.
- Create and manage query bookmarks, and use [Built-in Queries](#) to dive deeper into possible attack paths.

Before you begin:

For Attack Path data ingestion to function as expected, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
  - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** [scan template](#). This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

**Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

- [Tenable Identity Exposure](#) SaaS deployed.

**Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Tenable Exposure Management. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:
  - Have at least 40% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.



- An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
- When using Tenable Identity Exposure, enable [privileged analysis](#). This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
- A scan frequency of at least once a week.
- Configure Tenable OT Security.
- Configure Tenable Attack Surface Management and [configure the application for use with Tenable Vulnerability Management](#). This ensures that usable data gets pulled into Tenable Exposure Management.

To access the **Top Attack Paths** tab:

1. Do one of the following:

- In the left navigation menu, click **Attack Path > Attack Paths**.
- At the top of the [Attack Path](#) page, click the **Attack Paths** tab.

The **Top Attack Paths** tab appears.

**Custom Queries**

- Attack Path Query Builder**  
Show attack paths from an asset towards another asset
- Asset Query Builder**  
Search for group of assets or a specific one

**Query Library**

- Bookmarks**  
1 search queries
- Active Directory Misconfigurations**  
8 search queries
- Cloud**  
7 search queries
- Cloud Identities**  
2 search queries
- Common Vulnerabilities**  
12 search queries
- Credentials**  
3 search queries

**Top Attack Paths**

Choose your filter... [Apply] [Menu]

Target ACR > 8 | Vulnerability Management | Identity Exposure | Web Application Scanning | OT Security | Cloud Security | Attack Surface Management

0 Selected | [+ Export Selected (0)] [- Export All] | Page 1 of 10 | 1 to 25 of 229

<input type="checkbox"/>	View Graph	Name	Path Priority Rating	Nodes	Actions
<input type="checkbox"/>		Exposed External Remote Services Allow Internet Access to Cloud Resources [AI]	High		
<input type="checkbox"/>		ws2 to Administrator [New]	High		
<input type="checkbox"/>		An attacker can move from ws1 to DC1 by exploiting CVE-2023-36025 [AI]	High		
<input type="checkbox"/>		An attacker can move from ws1 to DC1 by exploiting CVE-2022-41076 [AI]	High		
<input type="checkbox"/>		Attacker can gain access to DC1 by exploiting CVE-2024-21412 [AI]	High		
<input type="checkbox"/>		Windows workstation ws1 reaches into domain controller DC1 by exploiting CVE-2... [AI]	High		
<input type="checkbox"/>		Attacker can gain access to DC1 by exploiting CVE-2023-36884 [AI]	High		
<input type="checkbox"/>		ws1 can be used to access domain admin credentials [AI]	High		
<input type="checkbox"/>		Public internet leads to data exfiltration from tenable-attack-path-close-bucket ... [AI]	High		

**Tip:** To view the source of an attack path detection, on the [Attack Technique Details](#) page, view the applicable attack path techniques' [Related Sources](#).



By default, the **Top Attack Paths** list appears, which lists the top attack paths leading to critical assets.

In this list, you can:

- Filter the list:

**Tip:** Below the search box, click a quick filter button to automatically filter the list by the selected item.

- a. At the top of the list, click inside the search box.

The **Choose your filter** drop-down box appears where you can choose a filter by which to filter the top attack path list. These include, but are not limited to:

Filter	Description
<b>Name</b>	Filters by the attack path name.
<b>Summary</b>	Filters by the attack path summary text.
<b>Priority</b>	Filters by priority: critical, high, medium, or low.

- b. Select the filter you want to use to filter the list.

The **Choose operator** drop-down box appears.

- c. Select the operator you want to use to filter the list.

The **Choose value** drop-down box appears.

- d. Select the value you want to use to filter the list.

- e. Click **Apply**.

Tenable Exposure Management filters the list based on your criteria.

- Show/hide columns in the list:

- a. In the upper-right corner of the list, click the  button.

A drop-down menu appears.

- b. Select or deselect the check box next to the column you want to show or hide in the list.



The list updates based on your selection.

- Export one or more attack paths:

Do one of the following:


- In the list, next to the attack path you want to export, click the  button.

A menu appears.

- a. Click **Export as CSV**.


- In the list, select the check box next to each attack path you want to export.

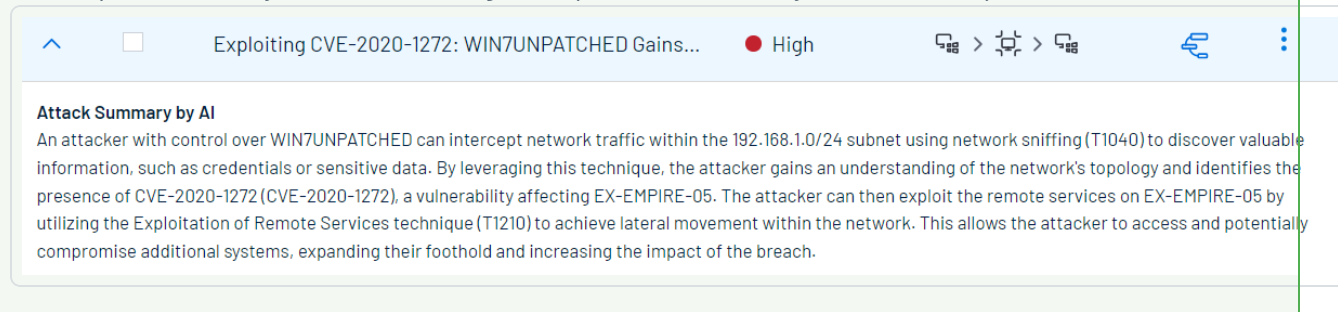
- a. At the top of the list, click  **Export Selected**.

- To export all attack paths, at the top of the list, click  **Export All**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.


- View the following attack path information:

**Tip: (Not supported in [FedRAMP](#) environments)** Click the  button in any row to expand the full attack path summary details, including an AI powered summary of the attack path.




**Attack Summary by AI**

An attacker with control over WIN7UNPATCHED can intercept network traffic within the 192.168.1.0/24 subnet using network sniffing (T1040) to discover valuable information, such as credentials or sensitive data. By leveraging this technique, the attacker gains an understanding of the network's topology and identifies the presence of CVE-2020-1272 (CVE-2020-1272), a vulnerability affecting EX-EMPIRE-05. The attacker can then exploit the remote services on EX-EMPIRE-05 by utilizing the Exploitation of Remote Services technique (T1210) to achieve lateral movement within the network. This allows the attacker to access and potentially compromise additional systems, expanding their foothold and increasing the impact of the breach.

- **View Graph** – Click the  button in the row of any attack path for which you want to view a graphical representation the attack path. For more information, see [View the Attack Path Graph](#).
- **Name** – The name of the attack path.
- **Path Priority Rating** – The priority of an attack path. Tenable Exposure Management calculates the PPR based on the relative number of attack paths to critical assets.



Tenable Exposure Management categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**.

- **Nodes** — A visual representation of the nodes involved in the attack path that indicates the node type and the order in which the nodes might be accessed.
- **Actions** — Click the  in the row of any attack path to perform the following actions:
  - **View Attack Techniques** — Click to navigate directly to the [Top Attack Techniques](#) page, filtered by techniques related to the selected attack path.
  - **Export as CSV** — Click to export the attack path in CSV format. Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

On the **Top Attack Paths** tab, you can also:

- Use the [Attack Path Query Builder](#) to generate a custom attack path query.
- Use the [Asset Query Builder](#) to generate a custom query for one or more assets or asset groups.
- Use a [Built-in Query](#) in the **Query Library** to generate a pre-configured query.

## Generate an Attack Path Query with the Attack Path Query Builder

You can use the **Attack Path Query Builder** to generate an attack path from one asset to another. You can create a query from a specific node or asset origin, and then specify the target to which you want to compare.



## Query builder

[Back to queries](#)

Standard queries

**Attack Path Query Builder**

Search

Please add parameters first

☒ Standard

☐ Blast Radius ?

☐ Asset Exposure ?

Source

+

Swap

Target

+

Attack Technique

+

**Tip:** To generate an attack path using a built-in query, see [Generate an Attack Path with a Built-in Query](#).

To generate a custom attack path query:

1. Access the [Top Attack Paths](#) tab.
2. In the **Custom Queries** section, click **Attack Path Query Builder**.

The **Query Builder** pane appears.

3. In the **Source** box, click the **+** button.

The source options appear.





4. For each source you want to include in the query:

a. Select the radio button next to the type of origin you want to use for the query:

- **Asset type** — Generate a query based on a certain type of asset.
- **Specific asset** — Generate a query based on a specific asset.

b. In the text box, type the asset type or specific node/asset you want to use for the query.

c. (Optional) To apply filters to the origin:

i. Click the  button.

The **Filters** window appears.

ii. In the **Parameter** drop-down, select the parameter by which you want to filter the origin.

iii. In the **Operator** drop-down, select the operator to apply to the parameter.

iv. In the text box, type or select the value or values you want to use for the filter.

**Note:** The values you can use differ depending on the parameter you selected.

v. Click **Apply and search**.

Tenable Exposure Management applies the filter to the origin.

5. In the **Target** section, click the  button.

The target options appear.

6. For each target you want to include in the query:

a. Select the radio button next to the type of target you want to use for the query:

- **Asset type** — Generate a query based on a certain type of asset.
- **Specific asset** — Generate a query based on a specific asset.

b. In the text box, type the asset type or specific node/asset you want to use for the query.

c. (Optional) To apply filters to the target:



- i. Click the  button.


The **Filters** window appears.

- ii. In the **Parameter** drop-down, select the parameter by which you want to filter the target.
- iii. In the **Operator** drop-down, select the operator to apply to the parameter.
- iv. In the text box, type or select the value or values you want to use for the filter.

**Note:** The values you can use differ depending on the parameter you selected.

- v. Click **Apply and search**.

Tenable Exposure Management applies the filter to the target.

7. (Optional) Click  Swap to swap between **Source** and **Target** assets.

8. In the **Attack Technique** section, click the  button.

A text box in which you can search for and select techniques appears.

9. In the **Technique** box, type or select a specific attack technique.

Tenable Exposure Management updates the list based on the search criteria. For more information on supported techniques, see [Supported Attack Path Techniques](#).

10. (Optional) Click  **Add a Technique** to add additional techniques.

**Note:** Tenable Exposure Management enables  **Add a Technique** only after you add an initial technique.

**Caution:** You must add techniques to your query in the order in which they appear in an attack path. Tenable Exposure Management does not provide query results for incorrectly ordered techniques.

11. Click **Search** .

Tenable Exposure Management returns any attack paths that match the query you created. For more information on interacting with the data, see [Interact with Attack Path Query Data](#).



12. (Optional) To reset the query pane, at the top of the pane, click the  button.

Tenable Exposure Management resets the selections within the pane.


## (Optional) Save your Query as a Preset/Bookmark

Once you've built your custom query, you can save it as a preset, where you can then access it as a bookmark when [creating new built-in](#) attack path queries.

To save your query as a preset:

1. At the top of the pane, click the  button.

The **Save as preset** window appears.

2. In the **Name of preset** text box, type a name for the query.
3. In the **Description of preset** text box, type a description of the query.
4. Click **Save preset** .

Tenable Exposure Management saves the query as a preset. You can access your saved queries in the **Bookmarks** section of the [Query Library](#).

What to do next:

[Interact](#) with the attack path data provided by the query.

## Generate an Asset Exposure Query

You can generate a query to view your **Asset Exposure**, which helps you to visualize an attack path from multiple assets down to one asset.

To generate an Asset Exposure query:

1. Access the [Top Attack Paths](#) tab.
2. In the **Custom Queries** section, click **Attack Path Query Builder**.

The **Query Builder** pane appears.

3. Select the **Asset Exposure** radio button.



The **Source** options auto-fill.

### Query builder

[Back to queries](#)

Standard queries

#### Asset Exposure graph

Search

Please add parameters first

☐ Standard

☐ Blast Radius

☒ Asset Exposure

Source

☒ Asset type

☐ Specific asset

AllAssets

1

+ Add a Source

↓

Target

+

- Click the **Target** drop-down, and, for each target you want to include in the query:

- 272 -



- a. Select the radio button next to the type of target you want to use for the query:
  - **Asset type** — Generate a query based on a certain type of asset.
  - **Specific asset** — Generate a query based on a specific asset.
- b. In the text box, type the asset type or specific node/asset you want to use for the query.
- c. (Optional) To apply filters to the target:

- i. Click the  button.

The **Filters** window appears.

- ii. In the **Parameter** drop-down, select the parameter by which you want to filter the target.
- iii. In the **Operator** drop-down, select the operator to apply to the parameter.
- iv. In the text box, type or select the value or values you want to use for the filter.


**Note:** The values you can use differ depending on the parameter you selected.

- v. Click **Apply and search**.


Tenable Exposure Management applies the filter to the target.

5. Click **Search** .

Tenable Exposure Management returns any attack paths that match the query you created. For more information on interacting with the data, see [Interact with Attack Path Query Data](#).

6. (Optional) To save the query as a preset, at the top of the pane, click the  button.

The **Save as preset** window appears:

- a. In the **Name of preset** text box, type a name for the query.
- b. In the **Description of preset** text box, type a description of the query.
- c. Click **Save preset** .

Tenable Exposure Management saves the query as a preset.



**Tip:** When you save a query as a preset, you can use it as a filter on the [Top Attack Paths](#) tab.

What to do next:

[Interact](#) with the attack path data provided by the query.

## Generate a Blast Radius Query

In the **Attack Path** section, you can generate a query to view **Blast Radius**, which helps you to visualize an attack path from one asset to multiple other assets.

To generate a Blast Radius query:

1. Access the [Top Attack Paths](#) tab.
2. In the **Custom Queries** section, click **Attack Path Query Builder**.

The **Query Builder** pane appears.

3. Select the **Blast Radius** radio button.

The **Target** options auto-fill.

Query builder

[Back to queries](#)

Standard queries

**Blast Radius**

Search

Please add parameters first

☐ Standard

☒ Blast Radius ?

☐ Asset Exposure ?

Source

+

↓

Target

^

☒ Asset type

☐ Specific asset

AllAssets

1

+ Add a Target

4. Click the **Source** drop-down, and, for each source you want to include in the query:
  - a. Select the radio button next to the type of source you want to use for the query:
    - **Asset type** — Generate a query based on a certain type of asset.
    - **Specific asset** — Generate a query based on a specific asset.

- 275 -



- b. In the text box, type the asset type or specific node/asset you want to use for the query.
- c. (Optional) To apply filters to the source:

- i. Click the  button.

The **Filters** window appears.

- ii. In the **Parameter** drop-down, select the parameter by which you want to filter the origin.
- iii. In the **Operator** drop-down, select the operator to apply to the parameter.
- iv. In the text box, type or select the value or values you want to use for the filter.


**Note:** The values you can use differ depending on the parameter you selected.

- v. Click **Apply and search**.


Tenable Exposure Management applies the filter to the origin.

5. Click **Search** .

Tenable Exposure Management returns any attack paths that match the query you created. For more information on interacting with the data, see [Interact with Attack Path Query Data](#).

6. (Optional) To save the query as a preset, at the top of the pane, click the  button.

The **Save as preset** window appears:

- a. In the **Name of preset** text box, type a name for the query.
- b. In the **Description of preset** text box, type a description of the query.
- c. Click **Save preset** .

Tenable Exposure Management saves the query as a preset.

What to do next:

[Interact](#) with the attack path data provided by the query.

Interact with Attack Path Query Data





After running an [Attack Path Query](#), Tenable Exposure Management displays the results associated with your query. From here, you can drill-down and interact with the data to gain further insights into the attack path, the nodes techniques involved, and how these could affect your overall security.

To view and interact with attack path query data:

1. Create one of the following query types:
  - Use the [Query Builder](#) to generate a custom query.
    - Generate an [Asset Exposure](#) query to visualize attack paths from multiple assets down to one asset.
    - Generate a [Blast Radius](#) query to visualize attack paths from one asset to multiple other assets.
  - Use a [Built-in Query](#) in the **Query Library** to generate a pre-configured query.

The **Query Result** page appears.

### Query Result (10 Attack Paths)

Apply ⌵

Target ACR > 8 Vulnerability Management Identity Exposure Web Application Scanning OT Security Cloud Security Attack Surface Management

0 Selected ↔ Export Selected (0) ↔ Export All 1 to 10 of 10 Find all attack paths

<input type="checkbox"/>	View Graph	Name	Path Priority Rating ⓘ	Nodes	Actions
>	<input type="checkbox"/>	SSH Authorized Keys from admin to yossiclust3r-ng1-Node <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮
>	<input type="checkbox"/>	SSH Authorized Keys from admin to yossiclust3r-ng1-Node <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮
>	<input type="checkbox"/>	SSH Authorized Keys from admin to cg-ubuntu-ec2-1 <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮
>	<input type="checkbox"/>	SSH Authorized Keys from admin to vulnapplication-ng-405f9ea9-Node <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮
>	<input type="checkbox"/>	SSH Authorized Keys from admin to vulnapplication-ng-405f9ea9-Node <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮
>	<input type="checkbox"/>	SSH Authorized Keys from admin to yossiclust3r-ng1-Node <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮
>	<input type="checkbox"/>	SSH Authorized Keys from admin to web01-research-blackhat <span>AI</span>	● Medium	🔑 > 📁 > 📁	⋮

1. On the **Query Result** page, you can:

**Note:** Because the options and data in this section depend on the type of query you run, some items listed below may not be available for your query.



- Filter the list of attack paths:

**Tip:** Below the search box, click a quick filter button to automatically filter the list by the selected item.

- a. At the top of the list, click inside the search box.

The **Choose your filter** drop-down box appears.

- b. Select the filter you want to use to filter the list.

The **Choose operator** drop-down box appears.

- c. Select the operator you want to use to filter the list.


The **Choose value** drop-down box appears.

- d. Select or type the value you want to use to filter the list.


- e. Click **Apply**.


Tenable Exposure Management filters the list based on your criteria.

- View a list of attack paths that match your query. This table includes the following attack path information:



Column	Description
<b>View Graph</b>	Click the  button to view the attack path in a graphical format. For more information, see <a href="#">View the Attack Path Graph</a> .
<b>Name</b>	The attack path name.
<b>Path Priority Rating</b>	A prioritization metric for attack paths based on the exposure of the source, criticality of the target and the number of steps of the attack path. Higher PPR indicates higher risk.
<b>Nodes</b>	The asset nodes associated with the attack path. If there are multiple nodes within the attack path, Tenable Exposure Management inserts directional arrows to show the direction of the path to and from each node.



	<b>Tip:</b> Hover your mouse cursor over the icon in this column to view the full name of the node type.
<b>Actions</b>	<p>Click the  button to view available actions.</p> <p>A menu appears:</p> <ul style="list-style-type: none"><li>◦ Click <b>View Attack Techniques</b> to navigate directly to the <a href="#">Top Attack Techniques</a> page filtered by the selected attack path.</li><li>◦ Click <b>Export as CSV</b> to export the attack path information as a .csv file.</li></ul>

- **(Not supported in [FedRAMP](#) environments)** Click the  button to expand an AI generated summary of the attack path.
- Export one or more attack paths from the list:

Do one of the following:

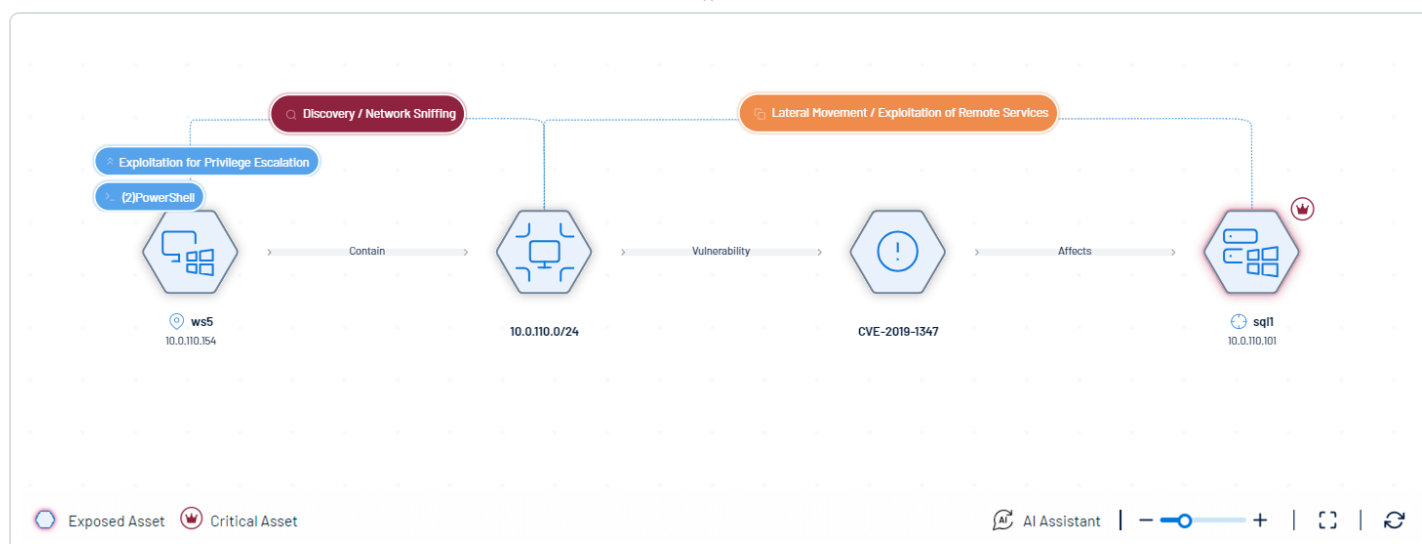
- To export individual attack paths:
  - a. In the list, select the check box next to each asset you want to export.
  - b. At the top of the list, click  **Export Selected**.
- To export all attack paths in the list:
  - a. At the top of the list, click  **Export All**.

Tenable Exposure Management downloads the list of selected attack paths as a .csv file.

## View the Attack Path Graph

When you click **View Graph** in the **Query Result** list, Tenable Exposure Management shows a graphical representation of the selected attack path.

**Note:** Because the options and data in this section depend on the type of query you run, some items listed below may not be available for your query.



In this section you can:

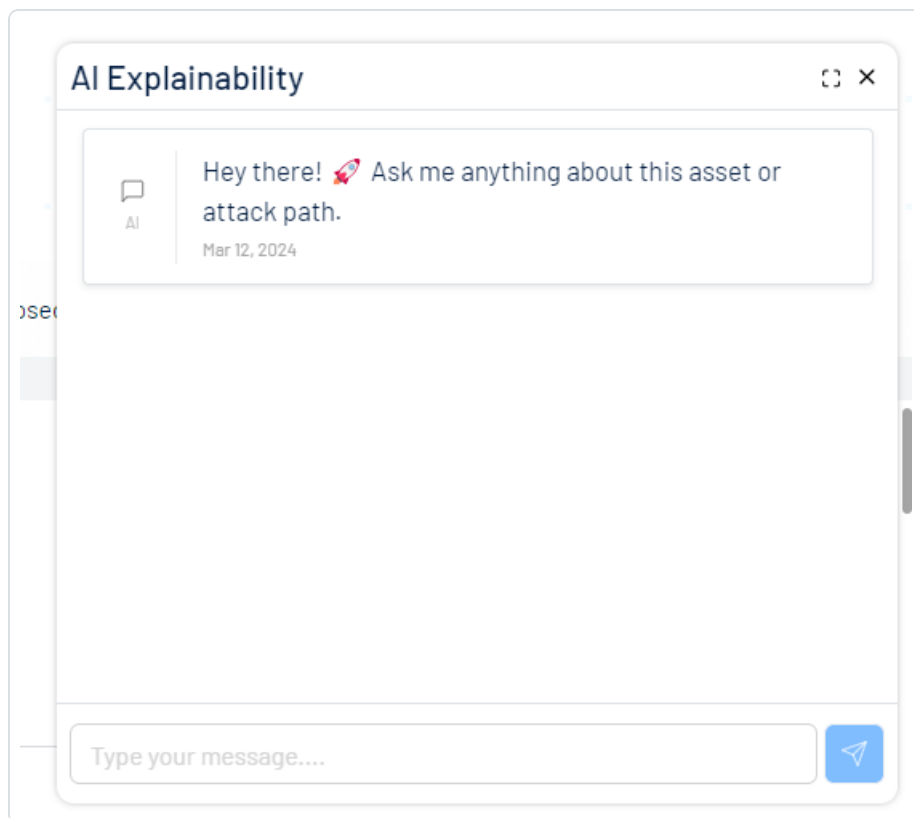
- **(Not supported in [FedRAMP environments](#))** At the top of the graph, click the button to expand an AI generated summary of the attack path. Here, you can also view a list of **Related Sources** for the attack path. This section displays information about the data sources used or seen within this specific attack path.

**Note:** While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

- View icons that represent the steps within the attack path, or the assets that match your query parameters.
    - Where applicable, view color coded steps and assets:
      - Technique segments color coded by priority (for example, a technique in red should be prioritized above a technique in orange).
- Note:** Informational attack paths, or attack paths without a priority, appear in blue.
- Exposed assets highlighted in red.
  - Critical assets highlighted by the icon.
  - Click on a step or an asset to [view additional details](#) for that item.





- Where applicable, view direction arrows and other indicators that show the source, direction, and target of the attack path.
- **(Not supported in [FedRAMP environments](#))** Click **AI Assistant** to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.



Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path.

For more information about AI explainability, how to use it, and its limitations, see the [Generative AI Best Practices Guide](#).

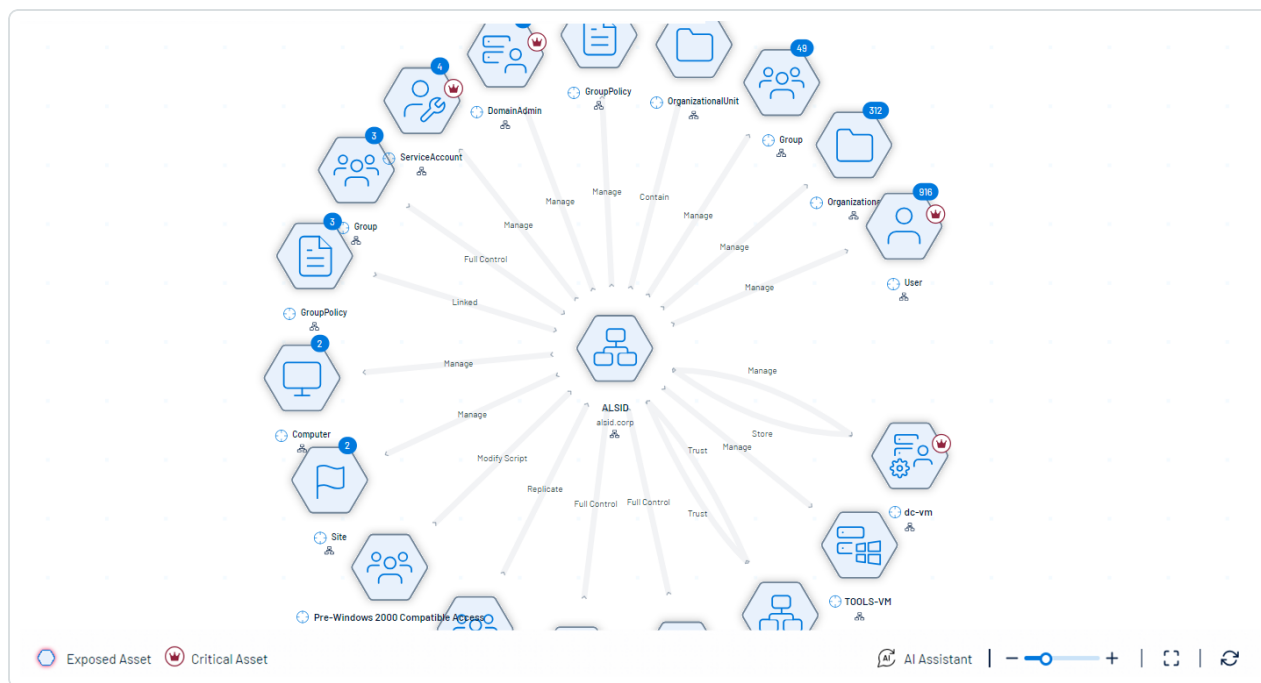
- Use your mouse cursor, the zoom slider, or the + and - buttons in the lower-right corner of the graph to zoom the graph in and out.
- Click the  button to enable or disable full screen view.
- Click the  button to reset the graph.



- Right-click on a step or an asset node to open a menu with additional options:
  - **(Not supported in [FedRAMP](#) environments) Ask AI About This Node** — Click to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.

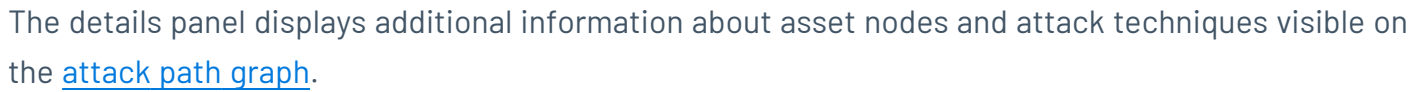
Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path. For more information about AI explainability, how to use it, and its limitations, see the [Generative AI Best Practices Guide](#).

- **Expand Node** — Click to expand a full view of all items related to the asset node.



- **Blast Radius** — Click to open a blast radius query, where the selected node is the source of the attack path. For more information, see [Generate a Blast Radius Query](#).
- **Asset Exposure** — Click to open an Asset Exposure query, where the selected node is the target of the attack path. For more information, see [Generate an Asset Exposure Query](#).

## View Node / Attack Details



1. Do one of the following:

- A panel appears at the bottom of the page with information about the node.

Node Details

\admin

Group

View Asset Details

Information

Related Techniques

Properties

ARN:

Cloud Provider: CloudProvider.aws

Cloud ID:

Cloud Security Labels: PII, Sensitive, Excessive, Admin, Access Keys, No ...

Relationships

Aws Account:

- **Open Ports** — The open ports on the asset.
- **ACR** — Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.
- **AES** — Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.
- **AVR** — The Asset Vulnerability Rating (AVR) is an aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on the asset.



- **NES** – The Node Exposure Score (NES) is a metric produced by Tenable Exposure Management to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
- **Sensors** – The sensor or sensors that detected the asset.
- Click an attack technique (i.e., step) on the canvas.

A panel appears with information about the technique such as:

- a **Description** of the technique.
- the **Tactics** used within the technique.
- any **Sub Techniques** used as part of the selected technique.

**Attack Details**

Tactics: **Privilege Escalation, Persistence** | Technique: **Account Manipulation** | Sub Technique: **SSH Authorized Keys** | Sub Technique ID [T1098.004](#)

**Information**

**Description**

Adversaries may modify the SSH `authorized_keys` file to maintain persistence on a victim host. Linux distributions and macOS commonly use key-based authentication to secure the authentication process of SSH sessions for remote management. The `authorized_keys` file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. This file is usually found in the user's home directory under `<user-home>/.ssh/authorized_keys`. Users may edit the system's SSH config file to modify the directives `PubkeyAuthentication`

**Related Sources**

- Tenable Cloud Security

Here you can:

- Click the **Technique ID** to navigate directly to the MITRE definition for that technique.
- View a list of **Related Sources** for the attack path technique.

**Note:** While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center





Without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

## Generate an Asset Query with the Asset Query Builder

You can use the **Asset Query Builder** to generate an interactive list of your nodes (assets and asset groups).

Query builder [Back to queries](#)

Standard queries

**Asset Query Builder**

Search

Please add parameters first

Asset

☒ Asset type ☐ Specific asset

Asset type (i.e: User)

+ Add a Asset

To generate a custom asset query:

1. Access the [Top Attack Paths](#) tab.
2. In the **Custom Queries** section, click **Asset Query Builder**.

The **Query Builder** pane appears.

3. For each asset you want to include in the query:



- a. Select the radio button next to the type of origin you want to use for the query:
  - **Asset type** — Generate a query based on a certain type of asset.
  - **Specific asset** — Generate a query based on a specific asset.
- b. In the text box, type the asset type or specific node/asset you want to use for the query.
- c. (Optional) To apply filters to the asset query:

- i. Click the  button.

The **Filters** window appears.

- ii. In the **Parameter** drop-down, select the parameter by which you want to filter the origin.
- iii. In the **Operator** drop-down, select the operator to apply to the parameter.
- iv. In the text box, type or select the value or values you want to use for the filter.

**Note:** The values you can use differ depending on the parameter you selected.

- v. Click **Apply and search**.

Tenable Exposure Management applies the filter to the asset query.

4. (Optional) Click  **Add an Asset** to add additional assets to the query.

5. Click **Search** .

Tenable Exposure Management returns any assets and/or asset groups that match the query you created. For more information on interacting with the data, see [Interact with Asset Query Data](#).

6. (Optional) To save the query as a preset, at the top of the pane, click the  button.

The **Save as preset** window appears:


- a. In the **Name of preset** text box, type a name for the query.
- b. In the **Description of preset** text box, type a description of the query.



- c. Click **Save preset** .

Tenable Exposure Management saves the query as a preset.

**Tip:** When you save a query as a preset, you can use it as a filter on the [Top Attack Techniques](#) tab.

7. (Optional) To reset the query pane, at the top of the pane, click the  button.

Tenable Exposure Management resets the selections within the pane.

What to do next:

[Interact](#) with the asset data provided by the query.

## Interact with Asset Query Data

After you run an [Asset Query](#), Tenable Exposure Management displays the results associated with your query. From here, you can drill down and interact with the data to gain further insights.

To view and interact with asset query data:

1. [Generate an Asset Query with the Asset Query Builder](#).

The **Query Result** page appears.



## Query Result (1101 Assets)



0 Selected | [Export Selected \(0\)](#) | [Export All](#)

<< < Page 1 of 45 > >> 1 to 25 of 1101

<input type="checkbox"/>	View Node	Name	Type	NES	AES	ACR	Action
<input type="checkbox"/>		arn:aws:s3:::tenable-attack-path-close-bucket		5	842	3	
<input type="checkbox"/>		832970976958\admin		0	0	0	
<input type="checkbox"/>		832970976958\aviv		3	586	3	
<input type="checkbox"/>		832970976958\yossi		3	586	3	
<input type="checkbox"/>		AWSServiceRoleForAutoScaling		0	0	0	
<input type="checkbox"/>		OrganizationAccountAccessRole		0	0	0	
<input type="checkbox"/>		test_role_terraform_inline		0	0	0	
<input type="checkbox"/>		ADM-Vuln-Administrator-Role		0	0	0	
<input type="checkbox"/>		test_role_terraform		0	0	0	


2. On the **Query Result** page, you can:

**Note:** Because the options and data in this section depend on the type of query you run, some of the following items may not be available for your query.

- View a list of assets that match your query. For example, if the query searches for workstations, the list displays all assets that have a **type** of **Workstation**. This table includes the following asset information:



Column	Description
<b>View Node</b>	Click the  button to view the asset nodes in a graphical format. For more information, see <a href="#">View Asset Nodes</a> .
<b>Name</b>	The asset name.
<b>Type</b>	The asset type, for example <b>Workstation</b> or <b>ServiceAccount</b> . <div><b>Tip:</b> Hover your mouse cursor over the icon in this column to view the full name of the asset type.</div>



<b>NES</b>	The Node Exposure Score (NES) is a metric produced by Tenable Exposure Management to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
<b>AES</b>	Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.
<b>ACR</b>	Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.
<b>Actions</b>	<p>Click the  button to view available actions.</p> <p>A menu appears:</p> <ul style="list-style-type: none"><li>◦ Click <b>Export as CSV</b> to export the asset information as a .csv file.</li></ul>

- Export one or more assets from the list:

Do one of the following:

- To export individual assets:
  - a. In the list, select the check box next to each asset you want to export.
  - b. At the top of the list, click  **Export Selected**.
- To export all assets in the list:
  - a. At the top of the list, click  **Export All**.

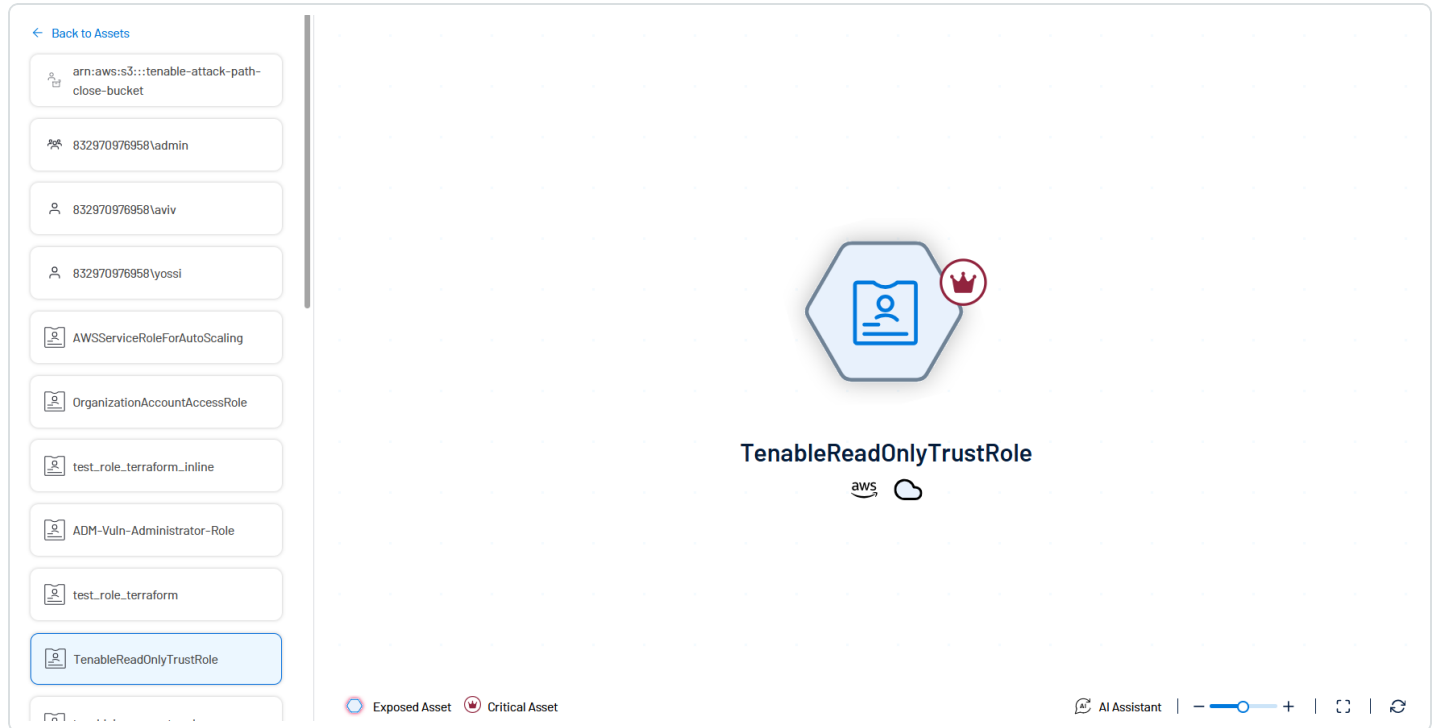
Tenable Exposure Management downloads the list of selected assets as a .csv file.

## View Asset Nodes



When you click **View Nodes** in the **Query Result** list, Tenable Exposure Management shows a graphical representation of the selected asset node.


**Note:** Because the options and data in this section depend on the type of query you run, some of the following items may not be available for your query.



In this section you can:

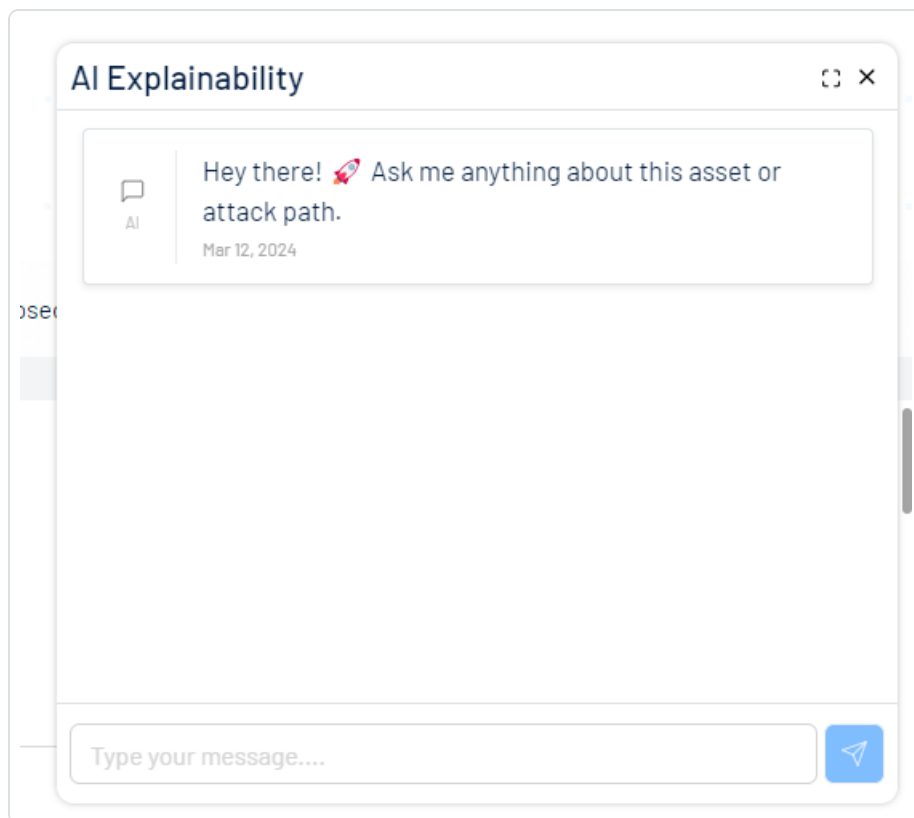
- (Optional) On the left side of the graph, in the asset list, select any asset for which you want to view the node.

**Note:** The assets in this list are the assets that match your asset query parameters.

- View an icon that represents the asset.
  - Where applicable, view color-coded assets:
    - Exposed assets highlighted in red.
    - Critical assets highlighted by the  icon.
- Click on a step or an asset to [view node details](#) for that item.





- Use your mouse cursor, the zoom slider, or the + and - buttons in the lower-right corner of the graph to zoom the graph in and out.
- **(Not available in [FedRAMP environments](#))** Click **AI Assistant** to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.



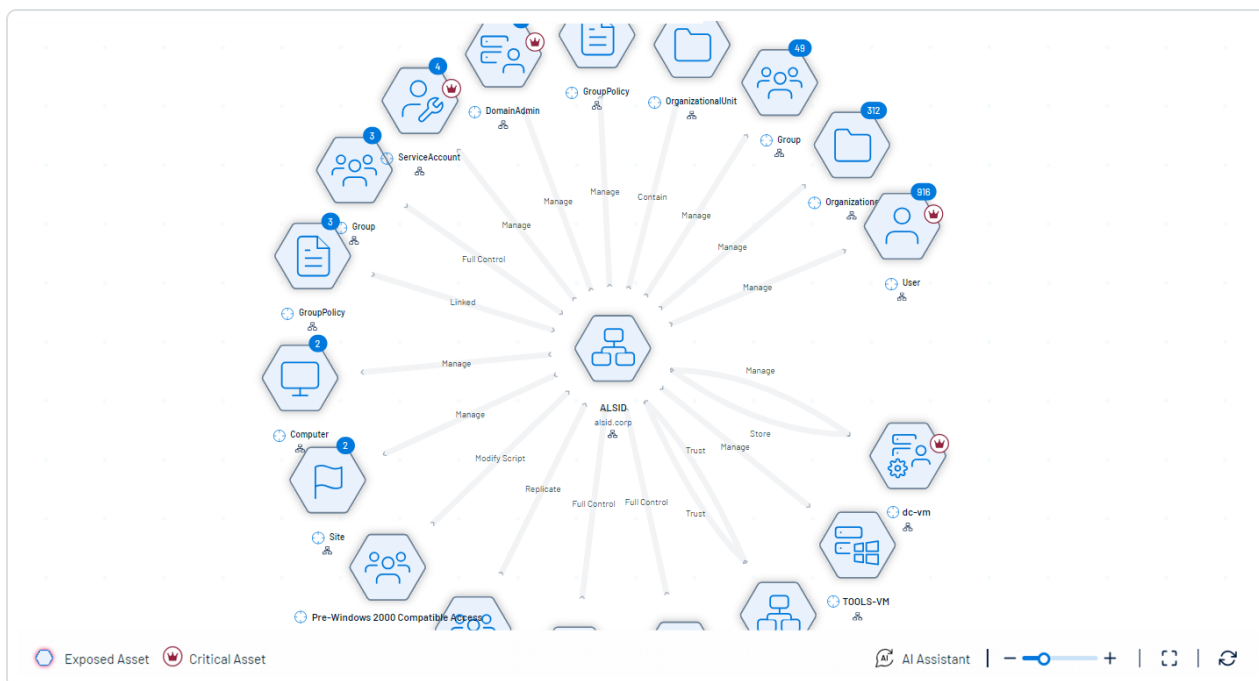
Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path.

For more information about AI explainability, how to use it, and its limitations, see the [Generative AI Best Practices Guide](#).

- Click the  button to enable or disable full-screen view.
- Click the  button to reset the graph.
- Right-click on a step or an asset node to open a menu with additional options:



- **(Not supported in [FedRAMP](#) environments) Ask AI About This Node** — Click to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.  
Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path. For more information about AI explainability, how to use it, and its limitations, see the [Generative AI Best Practices Guide](#).
- **Expand Node** — Click to expand a full view of all items related to the asset node.



- **Blast Radius** — Click to open a blast radius query, where the selected node is the source of the attack path. For more information, see [Generate a Blast Radius Query](#).
- **Asset Exposure** — Click to open an Asset Exposure query, where the selected node is the target of the attack path. For more information, see [Generate an Asset Exposure Query](#).

## View Node / Attack Details

The details panel displays additional information about asset nodes and attack paths visible on the [asset node graph](#).





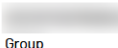
To view the information panel for a node or technique:


1. Click a node on the canvas.

A panel appears at the bottom of the page with information about the node.

**Tip:** In the upper-right corner, click **View Asset Details**  to view the node and its details directly on the [Asset Details](#) page.


**Node Details**

admin  
Group


View Asset Details 

InformationRelated Techniques

**Properties**



ARN: 

Cloud Provider: CloudProvider.aws

Cloud ID: 

Cloud Security Labels: PII, Sensitive, Excessive, Admin, Access Keys, No ...

**Relationships**

Aws Account:  

This information includes, but is not limited to:

- **Open Ports** — The open ports on the asset.
- **ACR** — Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.
- **AES** — Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.
- **AVR** — The Asset Vulnerability Rating (AVR) is an aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on the asset.
- **NES** — The Node Exposure Score (NES) is a metric produced by Tenable Exposure Management to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
- **Sensors** — The sensor or sensors that detected the asset.

## Generate an Attack Path with a Built-in Query



You can use Tenable-provided built-in queries to generate an attack path from one asset to another.



## Query Library



### Bookmarks

0 search queries



### Active Directory Misconfigurations

7 search queries



### Endpoint

3 search queries



### Exfiltration

3 search queries



### Network

1 search queries



### Permissions

3 search queries



### Ransomware

5 search queries



### Vectors

2 search queries





**Tip:** To generate your own custom query, see [Generate an Attack Path Query with the Attack Path Query Builder](#).

To generate a built-in query:

1. Access the [Top Attack Paths](#) tab.
2. In the **Query Library** section, click the tile that contains the search query you want to use. For more information, see [Query Types in the Query Library](#).

Tenable Exposure Management returns any attack paths that match the query you selected and the **Query Builder** appears. For more information on interacting with the data, see [Interact with Attack Path Query Data](#).

**Note:** If there are no matching attack paths, Tenable Exposure Management does not return any results for the query.

3. (Optional) Use the **Query Builder** to edit the built-in query you selected. For more information, see [Generate an Attack Path Query with the Attack Path Query Builder](#).

**Note:** If you edit a built-in query, your changes do not affect the query within the query library. Instead, you can save the new query as a preset, which appears in the **Bookmarks** tile in the [Query Library](#).

What to do next:

[Interact](#) with the attack path data provided by the query.

## Query Types in the Query Library

When generating an attack path from a [Built-in Query](#), you can use the following queries within the **Query Library**.

**Note:** Some query types may not be available for all users.

Tile	Query Types
<b>Bookmarks</b>	When a user saves a custom attack path query, Tenable Exposure Management saves the query in the <b>Bookmarks</b> section. Here, you can view the query, the user who created it, and select the bookmark



	<p>to use to generate an attack path query.</p> <p>For more information, see <a href="#">(Optional) Save your Query as a Preset/Bookmark</a>.</p>
<b>Active Directory Misconfigurations</b>	<ul style="list-style-type: none"><li>• <b>LAPS Password</b> – Users with permissions to read LAPS Passwords.</li><li>• <b>AdminSDHolder</b> – Users with write/full control access to AdminSDHolder objects.</li><li>• <b>Kerberos Delegation</b> – Users with permissions to perform Kerberos delegation.</li><li>• <b>Domain Admins vulnerable to Kerberos Delegation</b> – Domain Admins that are not part of Protected Users or has not delegated flag.</li><li>• <b>DNS Admins</b> – Users that are members of the DNS Admins group.</li><li>• <b>Reversible Password Hash</b> – Users whose password is stored in the Active Directory in reversible encryption format.</li><li>• <b>Password Not Expired</b> – Users whose password never expires.</li><li>• <b>Password Not Required</b> – Users who do not require a password for authentication.</li></ul>
<b>Cloud</b>	<ul style="list-style-type: none"><li>• <b>Exposed cloud storage</b> – Cloud storage that is exposed to the internet.</li><li>• <b>Computers vulnerable from cloud</b> – Computers that have management ports open from the Internet.</li><li>• <b>Publicly exposed workload leads to exfiltration</b> – A publicly exposed web application that leads to compromise of EC2 workload and access to data in S3 bucket.</li></ul>
<b>Common Vulnerabilities</b>	<ul style="list-style-type: none"><li>• <b>Bluekeep</b> – Computers that are vulnerable to CVE-2019-0708.</li><li>• <b>EternalBlue</b> – Computers that are vulnerable to CVE-2017-0144.</li></ul>



	<ul style="list-style-type: none"><li>• <b>log4shell</b> – Computers that are vulnerable to CVE-2021-44228.</li><li>• <b>PrintNightmare</b> – Computers that are vulnerable to CVE-2021-44228.</li><li>• <b>ProxyLogon</b> – Computers that are vulnerable to CVE-2021-26855.</li><li>• <b>Zerologon</b> – Computers that are vulnerable to CVE-2020-1472.</li></ul>
<b>Credentials</b>	<ul style="list-style-type: none"><li>• <b>Domain Admins password reuse</b> – Domain admin users whose passwords are shared by other users.</li><li>• <b>Cracked Passwords</b> – Passwords that could be cracked by an attacker.</li><li>• <b>Kerberoasting</b> – Users vulnerable to the Kerberoasting attack.</li></ul>
<b>Endpoint</b>	<ul style="list-style-type: none"><li>• <b>Computers that Cache Domain Admins</b> – Computers that are not Domain Controllers and cache the credentials of domain admin users.</li><li>• <b>Bitlocker</b> – Computers configured without Bitlocker.</li><li>• <b>Vulnerable registry service</b> – Computer services that can be altered by unprivileged Domain Users from the Registry.</li><li>• <b>Vulnerable service binaries</b> – Computer services that can be altered by unprivileged Domain Users from a binary file.</li><li>• <b>Services that Cache Domain Admins User</b> – Services that run under the context of domain admin users.</li></ul>
<b>Network</b>	<ul style="list-style-type: none"><li>• <b>Computers with SMBv1</b> – Computers with SMB version 1 enabled.</li><li>• <b>NBT-NS Poisoning</b> – LLMNR/NBT-NS Poisoning and SMB Relay techniques compromising domain admin users.</li></ul>
<b>Permissions</b>	<ul style="list-style-type: none"><li>• <b>Domain Admin Password Reset</b> – Users who have permissions to reset a domain admin user password.</li></ul>



	<ul style="list-style-type: none"><li>• <b>Critical Asset Policy Modification</b> – Users that have permissions to modify a Group Policy Object (GPO) that affects a Critical Asset.</li><li>• <b>Group Membership Modification</b> – Users that have permissions to modify group membership.</li><li>• <b>Network Shares Access</b> – Network shares accessible by the Everyone user group.</li></ul>
<b>Ransomware</b>	<div><b>Note:</b> The simulations used in these queries do not pose any risk of impact on your system.</div> <ul style="list-style-type: none"><li>• <b>WannaCry Ransomware Attack</b> – Search an attack with WannaCry TTPs, such as EternalBlue exploit.</li><li>• <b>Fancy Bear APT 28</b> – Search for an attack vector that mimics APT 28.</li><li>• <b>Maze Ransomware Attack</b> – Search an attack with Maze TTPs, such as unique WMI capabilities.</li><li>• <b>Ryuk Ransomware Attack</b> – Search an attack with Ryuk TTPs, such as unique encryption capabilities.</li><li>• <b>REvil Ransomware Attack</b> – Search an attack with REvil TTPs, such as unique evasion capabilities.</li><li>• <b>Lazarus Group</b> – Search for an attack vector that mimics Lazarus Group.</li><li>• <b>Petya Ransomware</b> – Search an attack vector where Petya Group used.</li></ul>
<b>Top Searches</b>	<ul style="list-style-type: none"><li>• <b>Computers with Domain Admin and Log4Shell</b> – Search for assets that are vulnerable to CVE-2021-44228 and cache the credentials of Domain Admin account</li><li>• <b>Network Shares that Can Be Accessed by Non-administrators</b> – Search for network shares with read/write access for a non-</li></ul>



	<p>administrative account</p> <ul style="list-style-type: none"><li>• <b>Services that Run As Domain Admin</b> – Search for system services that runs in the context of a Domain Admin account</li><li>• <b>Computers exposed to the internet via SMBv1</b> – Search for computers that were found with SMBv1 exposed to the internet.</li></ul>
<b>Vectors</b>	<ul style="list-style-type: none"><li>• <b>Domain Users to Domain Admins</b> – Users in the Domain Users group-escalating privileges to the Domain Admins group.</li><li>• <b>Workstations to Critical Assets</b> – An attack path from Workstations to Critical Assets.</li></ul>

## Supported Attack Path Techniques

As part of a typical attack, adversaries leverage different tools and techniques to accomplish their objectives. This event is known as Attack Path. An attack path contains one or more Attack Techniques, allowing the hacker to accomplish their objective. To see a full list of supported attack paths within Tenable Exposure Management, view the [Tenable Attack Path Techniques](#) list.

## Top Attack Techniques

As part of a typical attack, adversaries leverage different tools and techniques to accomplish their objectives. This event is known as Attack Path. An attack path contains one or more Attack Techniques, allowing the hacker to accomplish their objective. To see a full list of supported attack paths within Tenable Exposure Management, view the [Tenable Attack Path Techniques](#) list.

Every attack path contains one or more attack techniques. Every network includes multiple attack paths. Tenable helps you to focus on the most important paths by highlighting:

- Attack paths that lead to critical assets.
- Assets with an ACR greater than 7.
- Other Tenable defined static identifiers, such as **Domain Admins**.

An *attack technique* is a technique that exists in one or more attack paths that lead to one or more critical assets. The **Top Attack Paths** tab on the **Attack Path** page takes your data and pairs it with advanced graph analytics and the MITRE ATT&CK® Framework to create top attack techniques,





which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.

Before you begin:

For Attack Path data ingestion to function as expected, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
  - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** [scan template](#). This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

**Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

- [Tenable Identity Exposure](#) SaaS deployed.

**Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Tenable Exposure Management. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:
  - Have at least 40% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.
  - An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
  - When using Tenable Identity Exposure, enable [privileged analysis](#). This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.



- A scan frequency of at least once a week.
- Configure Tenable OT Security.
- Configure Tenable Attack Surface Management and [configure the application for use with Tenable Vulnerability Management](#). This ensures that usable data gets pulled into Tenable Exposure Management.
- At least one attack technique found within Tenable Exposure Management.
- At least one attack path generated within Tenable Exposure Management.
- Attack paths that use the previously mentioned attack technique and lead to at least one critical asset.

To access the **Top Attack Techniques** tab:

1. Do one of the following:
  - In the left navigation menu, click **Attack Path** > **Attack Techniques**.
  - At the top of the [Attack Path](#) page, click the **Attack Techniques** tab.

The **Top Attack Techniques** tab appears.

**Open Attack Techniques**  
140  
0 Critical  
2 High  
6 Medium  
138 Low

**Archived Attack Techniques**  
13418  
0 Critical  
0 High  
6 Medium  
13.4K Low

**Total Attack Techniques**  
13558  
0 Critical  
2 High  
6 Medium  
13.6K Low

### Top Attack Techniques

Choose your filter... Apply

0 Selected | Export Selected (0) | Export All | More

Page 1 of 6 | 1 to 25 of 140

	View Path	Priority	MITRE ATT&CK Id	Technique	Source	Target	Status	Actions
<input type="checkbox"/>		High	T1003	LSASS Memory	miles.demo.i...	DEMO\adminis...	To Do	
<input type="checkbox"/>		High	T1021	Remote Desktop Protocol	DEMO\it admin...	Domain Controllers 4	To Do	
<input type="checkbox"/>		Low	T1021	Remote Desktop Protocol	Users 2	In-dc.labnet...	To Do	
<input type="checkbox"/>		Low	T1133	External Remote Services	Internet-inf...	ec2-18-217-1...	To Do	
<input type="checkbox"/>		Low	T1210	Exploitation of Remote Services	172.26.42.0/24 Windows Servers 2	dcl.tenable....	To Do	
<input type="checkbox"/>		Low	T1210	Exploitation of Remote Services	172.26.42.0/24 Windows Servers 2	172.26.42.10...	To Do	

On the **Top Attack Techniques** tab, you can:



- On the left side of the page, view **Attack Techniques** tiles:
  - **Open Attack Techniques** – View the total number of open attack techniques within Tenable Exposure Management. Also, view the number of open techniques in each priority level.
  - **Archived Attack Techniques** – View the total number of archived attack techniques within Tenable Exposure Management. Also, view the number of archived techniques in each priority level.
  - **Total Attack Techniques** – View the total number of attack techniques within Tenable Exposure Management. Also, view the number of total attack techniques in each priority level.

**Deactivated Attack Techniques:** In cases where attack path data does not exist outside of the **Top Attack Techniques** list, Tenable Exposure Management automatically updates the [Log History](#) of the attack technique:

### Log History



02/19/2024  
16:34:15



State changed from **Open** to **Archived** by System due to a decrease in the number of attack paths from 1 to 0

- When a attack technique is not seen as part of any attack path, Tenable Exposure Management changes the attack technique **State** to **Archived**.
- When a attack technique cannot be found within the Attack Path Graph on the [Top Attack Paths](#) tab, Tenable Exposure Management changes the attack technique **State** to **Archived** and the **Status** to **Done**.

If at any point the attack technique is again seen as part of an attack path, Tenable Exposure Management automatically reactivates the attack technique **State** to **Open**.

Click on a tile to filter the **Top Attack Techniques** list by that type of technique.

- View the **Top Attack Techniques** list, where you can:



◦ Filter the **Top Attack Techniques** list:

- a. At the top of the **Top Attack Techniques** list, click inside the search box.

The **Choose your filter** drop-down box appears where you can filter the list.

Options include, but are not limited to:

Filter	Description
<b>Priority</b>	Filters by priority: critical, high, medium, or low.  <div><b>Note:</b> When calculating the priority, Tenable Exposure Management considers the following:<ul style="list-style-type: none"><li>• The number of attack paths where the attack technique is present compared to the total number of attack paths.</li><li>• The number of critical assets to which these attack paths lead compared to the total number of critical assets.</li><li>• The tactic used, for example, <b>lateral movement</b> or <b>privilege escalation</b>.</li></ul></div>
<b>Status</b>	Filters by status: <b>To Do</b> , <b>In Progress</b> , <b>In Review</b> , and <b>Done</b> .
<b>Source</b>	Filters by the attack path source.
<b>Target</b>	Filters by the attack path target.
<b>CVE</b>	Filters by specific CVEs.
<b>Mitigations</b>	Filters by mitigations for the attack techniques.
<b>Tactic</b>	Filters attack techniques with similar tactics.
<b>Technique</b>	Filters by attack techniques. For more information about attack techniques, view the <a href="#">Tenable Attack Path Techniques</a> list.

- b. Select the filter you want to use to filter the **Top Attack Techniques** list.

The **Choose operator** drop-down box appears.



- c. Select the operator you want to use to filter the **Top Attack Techniques** list.

The **Choose value** drop-down box appears.

- d. Select the value you want to use to filter the **Top Attack Techniques** list.

- e. Click **Apply**.

Tenable Exposure Management filters the **Top Attack Techniques** list based on your criteria.

- Show/hide columns in the **Top Attack Techniques** list:

- a. In the upper-right corner of the **Top Attack Techniques** list, click the  button.


A drop-down menu appears.

- b. Select or deselect the check box next to the column you want to show or hide in the list.

The **Top Attack Techniques** list updates based on your selection.

- [Export](#) an attack technique.
- Change the [status](#) of an attack technique.

**Tip:** See [View the Log History for an Attack Technique](#) for more information about attack technique statuses.

- [Archive](#) an attack technique.
- View the following attack technique information:
  - **View Path** – Click the  button in the row of any attack technique to navigate to the [Top Attack Paths](#) tab, where you can view a graphical representation of the attack path and interact with more attack path data.
  - **Priority** – The priority, or criticality, of the attack technique, for example, **Critical**.

**Note:** By default, the **Top Attack Techniques** list sorts attack techniques by highest priority first.



**Note:** When calculating the priority, Tenable Exposure Management considers the following:

- The number of attack paths where the attack technique is present compared to the total number of attack paths.
- The number of critical assets to which these attack paths lead compared to the total number of critical assets.
- The tactic used, for example, **lateral movement** or **privilege escalation**.

- **MITRE ATT&CK Id** – The MITRE ATT&CK identification number for the attack technique. Click an identification number to navigate directly to the MITRE ATT&CK listing for the attack technique.
- **Technique** – The MITRE ATT&CK technique associated with the attack technique.
- **Source** – The source of the attack technique.
- **To** – The target of the attack technique.
- **Status** – The status to indicate the action taken on the attack technique, for example, **In Progress**.

- Click on a technique to view additional [attack technique details](#).

## Attack Technique Details

You can view additional details for any attack techniques on the **Top Attack Techniques** tab on the **Attack Path** page.

To view additional details for an attack technique:

1. Access the [Top Attack Techniques](#) tab.
2. In the **Top Attack Techniques** list, click the attack technique for which you want to view additional details.



The attack technique details page appears.

[← Back to Top Attack Techniques](#)

## LSASS Memory

HIGH

Last update: 02/06/2025 04:34:22 | [Log History](#)

From [miles.demo.io.demo.io](#)

To [DEMO\administrator](#)

[View Attack Paths](#)

[Share](#)

### Details

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the t ...

### Choke Point Priority

HIGH

● 552 out of 955 Attack Paths leverage this attack and leads to 550 out of 550 Critical Assets

● Tactic: **Credential Access**

### Evidence

● Credentials Guard is disabled on the Computer [miles.demo.io](#)

● LSA Protection is disabled on the Computer [miles.demo.io](#)

● User [Administrator](#) is logged in to Computer [miles.demo.io](#)

On the attack technique page, you can:

- View the name and priority of the attack technique.
- View the date and time at which the attack technique was last updated. For example, a change in the status, priority, or state of a attack technique can change the **Last update** time.
- Click **Log History** to view the changes in the state, status, and priority of a attack technique. For more information, see [View the Log History for an Attack Technique](#).
- View information about source and target nodes within attack paths that exploit the attack technique.



- Click a node name to view additional details:

The node details panel appears.

The screenshot shows a user interface with a table on the left and a details panel on the right. The table has columns 'Name' and 'Type'. It contains one row with 'miles.demo.io.demo.io' and 'Windows Workstation'. A blue button with a link icon is next to the node name. The details panel, titled 'miles.demo.io Details', shows 'Windows Workstation' and a 'View Asset Details' button. It has two tabs: 'Information' (selected) and 'Related Techniques'. The 'Properties' section lists various attributes like Distinguished Name, Object SID, Asset ID, Name, ACR, AES, AVR, NES, Last Scanned, Last Observed, Last Licensed, Is Licensed, FQDN, IP Address, MAC Address, Network Interfaces, SMBv1 Enabled, LLMNR Enabled, and Operating System.

Name	Type
<a href="#">miles.demo.io.demo.io</a>	Windows Workstation

### miles.demo.io Details

Windows Workstation

[View Asset Details](#)

Information    Related Techniques

#### Properties

**Distinguished Name:** cn=miles,ou=workstations,ou=se demo environment as ...

**Object SID:** s-1-5-21-1141888507-2854189471-3097088611-1602

**Asset ID:** 1db5d659-0b54-467b-829c-cb463ee949b0

**Name:** miles.demo.io

**ACR:** 4

**AES:** 631

**AVR:** 10

**NES:** 6

**Last Scanned:** Wed Apr 17 2024

**Last Observed:** Wed Apr 17 2024

**Last Licensed:** Wed Apr 17 2024

**Is Licensed:** true

**FQDN:** miles.demo.io.demo.io

**IP Address:** 192.168.16.138

**MAC Address:** 00:50:56:A6:28:73

**Network Interfaces:** 1. IP: 192.168.16.138, Gateway: 192.168.16.1, Netw ...

**SMBv1 Enabled:** true

**LLMNR Enabled:** true

**Operating System:** Microsoft Windows 10 Pro Build 17134

**Vendor:** VMware, Inc.

[Cancel](#) [Export to CSV](#)

In the node details panel, you can:

- On the left side of the panel, select the node for which you want to view additional details.

The information on the right side of the panel updates accordingly.



**Tip:** Click the [link icon](#) button to view that node directly in the [Attack Path Graph](#).







- On the right side of the panel, click **View Asset Details** to navigate directly to the [Asset Details](#) page for that node.
- Click the **Information** tab to view further details about the node, including, but not limited to:
  - **NES** – The Node Exposure Score (NES) is a metric produced by Tenable Exposure Management to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
  - **Logged in Users** – Users currently logged into the node.
  - **Member of** – Lists the number of groups to which the node belongs.
  - **Related Types** – The node type as categorized by Tenable Exposure Management.





The information in this panel varies based on the node type, for example, **Computer** or **User**.

- Click the **Related Techniques** tab to view [Attack Path Techniques](#) associated with the node.
- Click **Export to CSV**  to export the node details in CSV format.
- Click **View Attack Paths** to navigate to the [Top Attack Paths](#) tab, where you can view a graphical representation of the attack path as well as interact with more attack path data.
- Click  **Share** to copy, send via email, or print the details of the attack technique:

Tenable Exposure Management displays the following menu:

Option	Description
	<ul style="list-style-type: none"><li>• Click the  button.</li></ul> <p>The attack technique page opens in your browser and the URL gets</p>



	copied to your clipboard.
	<ul style="list-style-type: none"><li>Click the  button.</li></ul> <p>Tenable Exposure Management opens your configured email with the URL to the attack technique details page.</p>
	<ul style="list-style-type: none"><li>Click the  button.</li></ul> <p>Tenable Exposure Management opens the <b>Print</b> window, where you can print the attack technique details page.</p>

- View a brief description of the **Details** of the attack technique.
- View the **Choke Point Priority** related to the attack technique.

**Tip:** A choke point is a place where potential attack paths merge together before reaching a critical asset. Tenable Exposure Management uses a **Choke Point Priority** metric to determine the criticality of choke points. Tenable recommends focusing on areas with higher choke points first, as remediating those will negate the largest number of critical items within your organization.

- View **Evidence** related to the attack technique.
- View **Related Sources** for the attack technique. This section displays information about the data sources used or seen within this specific attack technique.

**Note:** While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

- View **Mitigation Guidance** for the attack technique:
  - a. Click on an option to view further information steps you can take to mitigate the attack technique.
  - b. To view a step-by-step guide on how to mitigate the attack technique, click **Mitigation Guidelines**.

On the right side of the page, the **Mitigation Guidelines** panel appears, which includes a set of instructions you can follow to mitigate the attack technique and its related risk.



- View **Detection Guidance** for the attack technique.
- View **Related Threat Groups** associated with the attack technique.
- View **Related Malware and Tools** associated with the attack technique.
- View external **References**, where you can learn more about the attack technique.
  - a. Click a reference to navigate to that resource.


## Manage Attack Techniques

You can manage attack techniques in the following ways:


### Change the Status of an Attack Technique

You can change the status of one, several, or all attack techniques on the [Top Attack Techniques](#) tab on the **Attack Paths** page.

To change the status of an attack technique:

1. Access the [Top Attack Techniques](#) tab.
2. Do one of the following:
  - In the **Top Attack Techniques** list, next to the attack technique for which you want to change the status, click the  button.

A menu appears.

    - a. Click **Change Status**.
  - In the **Top Attack Techniques** list, select the check box next to each attack technique for which you want to change the status.
    - a. At the top of the list, click  **More**.

A menu appears.
    - b. Click **Change Status**.

A menu appears.



3. Click the status to which you want to change the attack technique, for example, **In Progress**.



Tenable Exposure Management updates the status of the attack technique.

### Export an Attack Technique

You can export one or more attack techniques on the [Top Attack Techniques](#) tab on the **Attack Paths** page. The export file includes information from the currently visible columns in the list. By default, Tenable Exposure Management also includes the following items in the export file:

- mitreURL
- state
- vectorCount

To export an attack technique:

1. Access the [Top Attack Techniques](#) tab.
2. Do one of the following:
  - In the **Top Attack Techniques** list, next to the attack technique you want to archive, click the  button.  
  
A menu appears.
    - a. Click **Export as CSV**.
  - In the **Top Attack Techniques** list, select the check box next to each attack technique you want to export.
    - a. At the top of the list, click  **Export Selected**.

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

### View the Log History for an Attack Technique

You can use the **Log History** page to view the following details for an attack technique:



- State changes, whether **Open** or **Archived**.
- Any change in the status: **To Do**, **In Progress**, **In Review**, Or **Done**.
- Changes in the priority level: **Critical**, **High**, **Medium**, or **Low**.

The priority of an attack technique can change for a number of reasons, including a change in the number of targets, sources, attack paths, or critical assets. Priority can also change if the target or source is renamed.

**Deactivated Attack Techniques:** In cases where attack path data does not exist outside of the **Top Attack Techniques** list, Tenable Exposure Management automatically updates the **Log History** of the attack technique:

### Log History

02/19/2024  
16:34:15




State changed from **Open** to **Archived** by System due to a decrease in the number of attack paths from 1 to 0

- When a attack technique is not seen as part of any attack path, Tenable Exposure Management changes the attack technique **State** to **Archived**.
- When a attack technique cannot be found within the Attack Path Graph on the [Top Attack Paths](#) tab, Tenable Exposure Management changes the attack technique **State** to **Archived** and the **Status** to **Done**.

If at any point the attack technique is again seen as part of an attack path, Tenable Exposure Management automatically reactivates the attack technique **State** to **Open**.


To view the log history of an attack technique:

1. Access the [Top Attack Techniques](#) tab.
2. In the **Top Attack Techniques** list, in the row of the attack technique for which you want to view the log history, click the  button.

A menu appears.

3. Click **Log History**.



The **Log History** page appears, where you can view a reverse chronological list of attack technique updates. To refresh the details on the page, click the  icon.

## Add and View Comments on an Attack Technique



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

Tenable Exposure Management allows you to add comments on any section of the attack technique details page and share it with other users in your organization. You can address your comment to a specific user and receive replies to your comment. Tenable Exposure Management also notifies you whenever someone replies to your comment or when new comments are added.

To comment on an attack technique:

1. Access the [Top Attack Techniques](#) tab.
2. Click the attack technique that you want to comment on.

The attack technique details page appears.


3. Do one of the following:
  - a. In the upper-right corner of the view, click the  button.
  - b. Scroll to the section on which you want to comment and click the  button.

The **Comments** pane appears.

4. In the text box, type your comment.

**Note:** You can send your comment to another user by prefixing @ before the user's email ID.


5. (Optional) To include a snapshot of the section on which you want to comment, select the **Include snapshot** check box.


6. Click the  button.

Tenable Exposure Management posts your comment and notifies other users about your comment.



## What to do next

Whenever someone posts a comment, the  icon in the upper-right corner shows a blue dot indicating that you have new comments.


To view the comments, click the  icon to open the **Comments** pane. When you click a comment, Tenable Exposure Management directs you to the section including the newly added comment.

### Archive an Attack Technique


You can archive one, several, or all attack techniques on the [Top Attack Techniques](#) tab on the **Attack Paths** page. By archiving an attack technique, you are effectively accepting the risk of the attack technique as part of attack paths within Tenable Exposure Management.

**Note:** Tenable Exposure Management automatically archives attack techniques that are no longer part of any attack paths. For more information, see [Log History](#).

To archive an attack technique:

1. Access the [Top Attack Techniques](#) tab.
2. Do one of the following:
  - In the **Top Attack Techniques** list, next to the attack technique you want to archive, click the  button.

A menu appears.

    - a. Click **Move to Archived**.
  - In the **Top Attack Techniques** list, select the check box next to each attack technique you want to archive.
    - a. At the top of the list, click  **More**.

A menu appears.
    - b. Click **Move to Archived**.

A confirmation message appears.



3. Click **Move to Archived**.

Tenable Exposure Management moves the attack technique to the **Archived Attack Techniques** section.

**Tip:** View the [Log History](#) to see the movement history of any given attack technique.

## MITRE ATT&CK Heatmap

The **MITRE ATT&CK Heatmap** tab on the **Attack Path** page provides a holistic view of your data based on tactics and techniques from the [Mitre Att&ck](#) framework.

Tenable Exposure Management presents the MITRE ATT&CK data in a table format that enables you to quickly prioritize and remediate critical vulnerabilities that are most relevant to your organization.

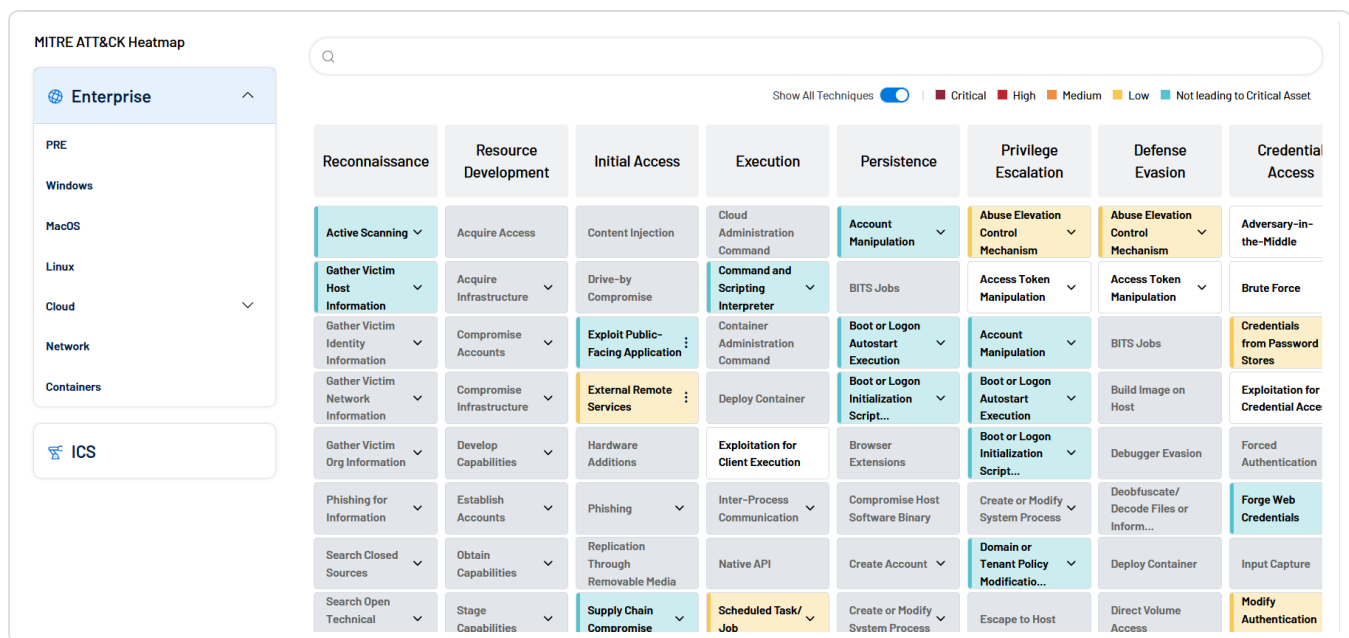
**Tip:** Check out the full list of [Attack Path Techniques](#) to view tactics, techniques, and the Tenable applications that trigger them.

To access the **MITRE ATT&CK Heatmap** tab:

1. Do one of the following:
  - In the left navigation menu, click **Attack Path > ATT&CK Heatmap**.
  - At the top of the [Attack Path](#) page, click the **ATT&CK Heatmap** tab.

The **MITRE ATT&CK Heatmap** tab appears.





2. Do one of the following:

- To view data based on enterprise tactics and techniques, in the left panel, click the **Enterprise** tab.
  - a. (Optional) Filter the table by platform type by selecting one of the available filters:
    - **PRE**
    - **Windows**
    - **MacOS**
    - **Linux**
    - **Cloud**
    - **Containers**
- To view data based on ICS (Industrial Critical Systems) tactics and techniques, in the left panel, click the **ICS** tab.

Tenable Exposure Management displays the relevant Mitre Att&ck data in a table format that includes the following details:



- Each column in the **MITRE ATT&CK Heatmap** table represents an enterprise tactic and its techniques. The column header shows the name of the enterprise tactic and the column shows its associated techniques.

For example, **Gather Victim Host Information**, **Gather Victim Identity Information**, and so on are enterprise techniques related to **Reconnaissance** enterprise tactic.

- Table cells are color-coded to indicate the following information:

■ Critical ■ High ■ Medium ■ Low ■ Not leading to Critical Asset

- Gray – Tenable does not currently support these techniques.
  - White – While Tenable supports these techniques and detects them, they are not relevant to your organization.
- Click on a cell to view top related attack paths and techniques:
    - a. Click the ▼ button.

A list of sub-techniques appears.

**Note:** If there are no sub-techniques for a technique, only the ⋮ icon is available.

- b. Click the ⋮ button.

A menu appears:

- **View Top Attack Techniques** – Navigate to the [Top Attack Techniques](#) page to view the attack techniques list filtered by the selected technique or sub-technique.
- **View Attack Paths** – Navigate to the [Top Attack Paths](#) page to view all possible attack paths for the selected technique or sub-technique.

**Tip:** Each menu option includes the number of attack techniques and attack paths available for the selected technique or sub-technique.

When viewing the **MITRE ATT&CK Heatmap** tab, you can do the following:



- Use the Search bar at the top of the table to search for specific techniques or sub-techniques.
- Click the **Show All Techniques** toggle to view only the cells that are color-coded by severity. This hides the white and gray cells in the heatmap table and shows only the techniques relevant to your organization.
- Click on a severity level to filter the page by severity.



# Tags

In Tenable Exposure Management, you can add your own business context to assets by tagging them with descriptive metadata. An asset tag is primarily composed of a *Category:Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*. For more information about tag structure, see [Tag Format and Application](#).

The **Tags** page allows you to view and manage all of your tags. You can quickly identify your number of tags, their related assets, and analyze the origin of each tag.

To access the **Tags** page:

1. In the left navigation menu, click **Tags**.
2. The **Tags** page appears.

Number of Tags

112

Number of Tag Categories

38

Search by Tag Category or Tag Value or Tag Category:Tag Value


New Tag

Tag Name	CES	Related Assets	Weakness Count	Last Updated	See Details
<div><div></div><div><div></div>Advance Search Dynamic tag: te...</div></div>	<div><div></div>87</div>	11,431	<div><div></div>26.5k</div>	25 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>Static_btest: test</div></div>	<div><div></div>87</div>	11,431	<div><div></div>26.5k</div>	24 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>sunny: testbug</div></div>	<div><div></div>322</div>	1,423	<div><div></div>26.2k</div>	22 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>Advance Search Dynamic tag: 10...</div></div>	<div><div></div>322</div>	1,423	<div><div></div>26.2k</div>	20 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>9th july: test clean - tal update</div></div>	<div><div></div>320</div>	1,422	<div><div></div>26.2k</div>	25 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>value tag with assets: Dynamic...</div></div>	<div><div></div>510</div>	3,465	<div><div></div>20.4k</div>	25 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>Advance Search Dynamic tag: As...</div></div>	<div><div></div>132</div>	5,336	<div><div></div>17.9k</div>	21 August 2025	<a href="#">See Details</a>
<div><div></div><div><div></div>New: Tag</div></div>	<div><div></div>132</div>	5,336	<div><div></div>17.9k</div>	21 August 2025	<a href="#">See Details</a>

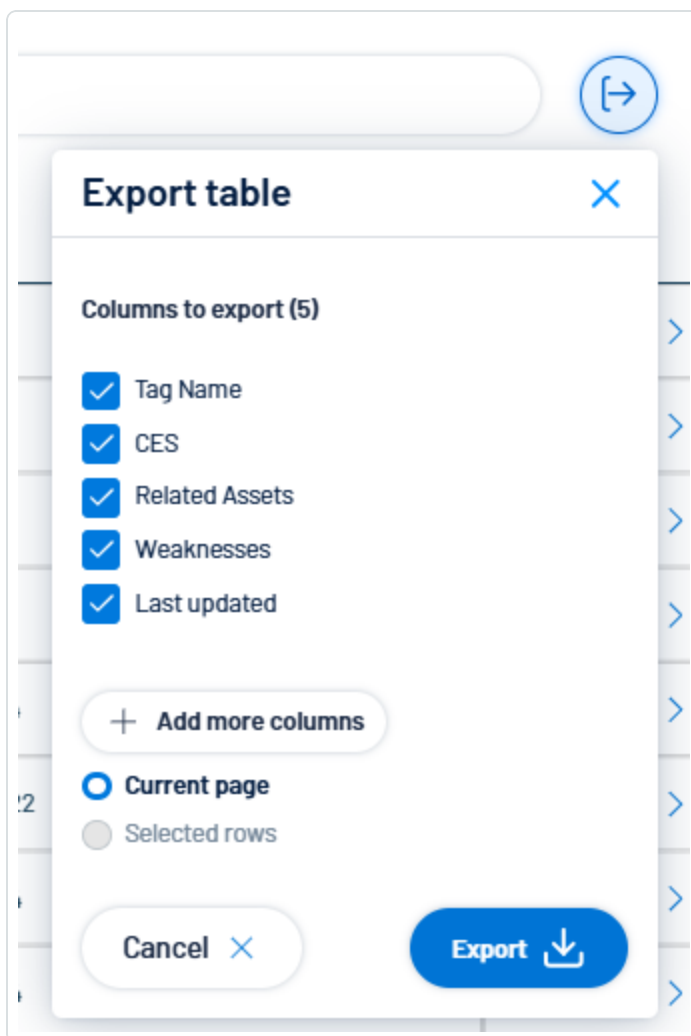
In the **Tags** view, you can:

- View the total number of tags within your container.
- View the total number of tag categories within your container.
- Manage your tags:



- [Create a New Tag](#)
- [Edit an Existing Tag](#)
- [Delete a Tag](#)
- Use the **Search** box to search for a specific tag value or tag category in the list.
- Export the table:
  - a. To the right of the search bar, click the  button.

The **Export table** plane appears.



- b. In the **Columns to export** section, select the check box for each column you want to include in the export file.



- c. (Optional) To include columns not currently in the table view, click **+ Add more columns**.

The **Add columns to export** plane appears.

- i. Select the check box for each additional column you want to include in the export file.
- d. In the rows section, ensure the **Current Page** radio button is selected.

**Tip:** Currently, you can only export the rows listed on the current page.


- e. Click **Export** .

Tenable Exposure Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

- Customize the columns in the table:

- a. Click **Columns** .

The **Customize columns** window appears.

- b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.
  - c. (Optional) In the **Show/Hide** section, select/deselect the check boxes to show or hide columns in the table.
  - d. (Optional) In the **Remove** section, click the  button to permanently remove a column from the table.
  - e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.

- i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

- ii. Select the check box next to any column or columns you want to add to the table.



iii. Click **Add**.

The column appears in the **Customize columns** window.

f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

g. Click  **Apply Columns**.

Tenable Exposure Management saves your changes to the columns in the table.

- View a list of your tags, including the following information:
  - **Tag name** — The name of the tag value or tag category.
  - **CES** — The [Cyber Exposure Score](#) for the tag value or tag category. The CES represents Cyber Exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for the assets to which the tag is applied. Higher CES values indicate higher risk.
  - **Related Assets** — The number of assets to which the tag is applied.
  - **Weakness Count** — The total number of weaknesses associated with the asset. For more information, see [Weaknesses](#).
  - **Last updated** — The date on which a user last updated the tag.
  - Click **See details** to view more details about a tag. For more information, see [Tag Details](#).

## Tag Format and Application

An asset tag is primarily composed of a *Category:Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*.

**Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category*, which you can use for all your tags.

## Static Tags vs. Dynamic Tags

When you [create a tag](#), you can choose between the following tag types:



- **static** – You must manually apply the tag to individual assets. Alternatively, you can manually apply an automatic tag to additional assets that may not meet the rules criteria for that tag.
- **dynamic** – Tenable Exposure Management automatically applies the tag to the assets on your instance that match the tag rules. When you create an automatic tag, Tenable Exposure Management applies that tag to all your current assets and any new assets added to your organization's account. Tenable Exposure Management also regularly reviews your assets for changes to their attributes and adds or removes automatic tags accordingly.

**Note:** When you [create](#) or [edit](#) a dynamic tag, Tenable Exposure Management may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

See the following examples for clarification:

Scenarios	Tag Type
You create a tag with <i>Location:Headquarters</i> as the <i>Category:Value</i> pair, but you do not add any tag rules. Later, you add the tag to assets located at your headquarters.	static
You create a tag with <i>Location:Headquarters</i> as the <i>Category:Value</i> pair, and you specify an IP address range in the tag rules. Tenable Exposure Management then automatically applies the tag to all existing or new assets within that IP address range.	dynamic

## Tag Details

In Tenable Exposure Management, you can view details for any tag value or category on the [Tags](#) page.

1. Access the [Tags](#) page.
2. In the row of the tag value or category for which you want to view details, click **See details**.





The tag details page appears.

[Back to Tags](#)

Delete

Edit

Tag Name

AWS Custom : neq-ap

Dynamic Tag

Cyber Exposure Score

402/1000

Included Assets

7.2k

Tag Preview

AWS Custom neq-ap

Sources

Tenable Vulnerability Management >

Last Modified

8 May 2023

Creation Date

8 May 2023

Creator

Jim One

Description

^ Included Assets

Search for asset name or asset ID

Name	Sources	Class	AES	Weaknesses	Top Attack Techniques	Top Attack Paths	Associated Ta...	Last Updated	See Details
sql1		Device	892	3.7k	2	1	8	24 December 2024	<a href="#">See Details &gt;</a>
srv1		Device	882	1.9k	8	1	6	25 December 2024	<a href="#">See Details &gt;</a>
tenable-ad-sql		Device	872	899	1	0	6	12 December 2024	<a href="#">See Details &gt;</a>
adfs1		Device	841	325	1	0	6	12 December 2024	<a href="#">See Details &gt;</a>
adcon1		Device	837	280	1	0	6	12 December 2024	<a href="#">See Details &gt;</a>

On the tag details page, you can:

- View the **Tag Name**.
- View the **Cyber Exposure Score** for the tag.
- View the number of **Included Licensed Assets** associated with the tag.
  - Click **See Details** to scroll down to the list of included assets.
- View the **Tag Preview**, where you can visualize the tag *category:value* pair.
- View the **Sources** where the tag originated.
  - Click the name of a data source to view that tag directly within its source application.
- View the date at which the tag value or tag category was **Last Modified**.
- View the **Creation Date** of the tag value or tag category.
- View the **Creator** of the tag value or tag category.
- View a **Description** of the tag value or tag category.
- View a list of the **Included Assets** associated with the tag. You can interact with this table the same way you interact with the table on the [Assets](#) page.



## Manage Tags

In Tenable Exposure Management, you can create and manage tags in the following ways:

### Create a New Tag

In the [Tags](#) view, you can create a static tag to apply to assets individually. You can also create an automatic tag by creating tag rules that Tenable Exposure Management uses to identify and tag matching assets.

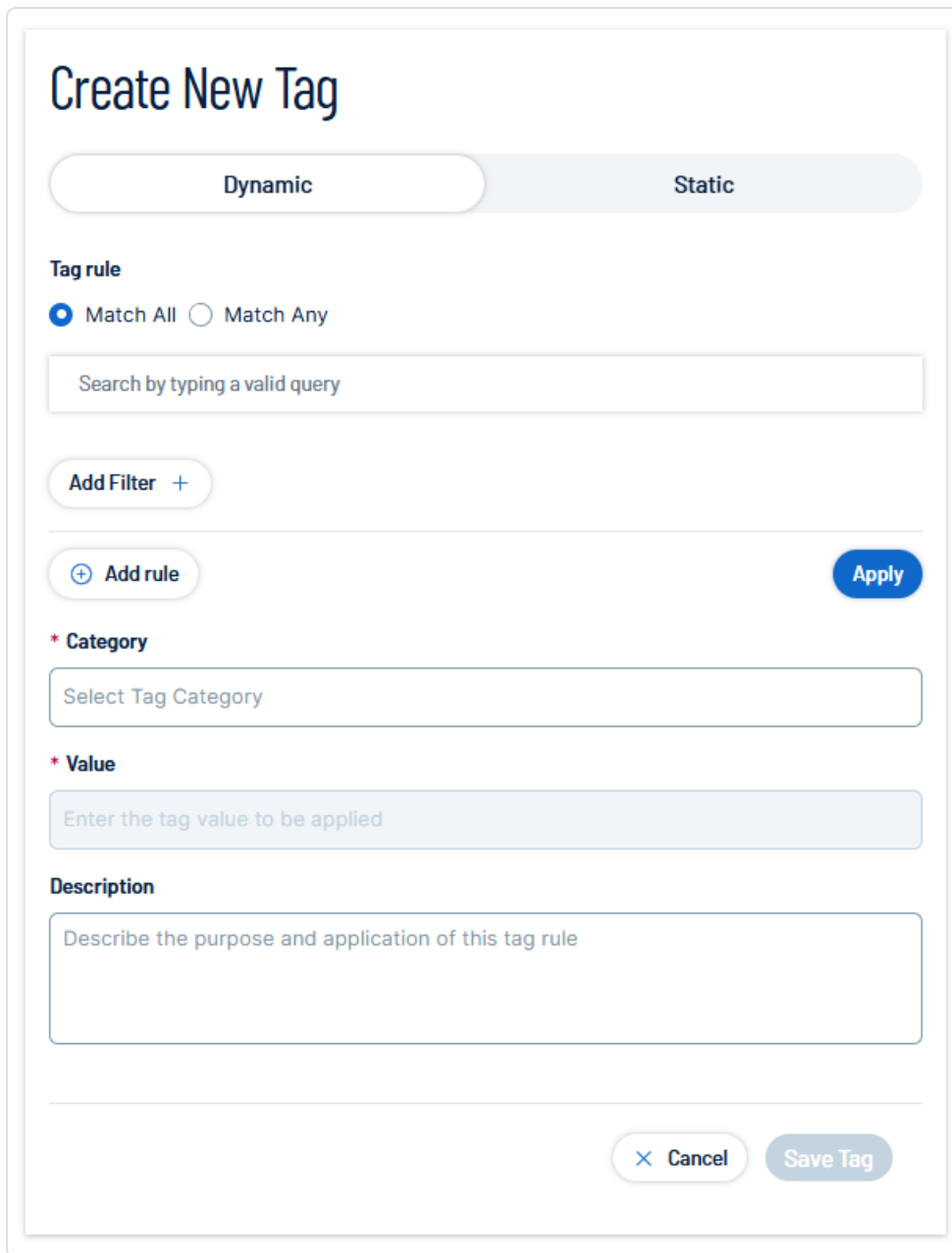
**Important!** Note the following tag creation limitations:

- A tag can include a maximum of 100 categories or a maximum of 100,000 tags per category, as configured by your organization.
- A tag can include a maximum of 1,000 rules.
- The request body of a tag cannot be greater than 1MB.

To create a tag:

1. Access the [Tags](#) page.
2. In the upper-right corner of the page, click **+ New tag**.

The **Create New Tag** page appears.



The image shows a 'Create New Tag' dialog box. At the top, there are two tabs: 'Dynamic' (selected) and 'Static'. Below the tabs, the 'Tag rule' section has two radio buttons: 'Match All' (selected) and 'Match Any'. A search bar with the placeholder text 'Search by typing a valid query' is below the radio buttons. Underneath the search bar is an 'Add Filter +' button. Further down, there is an 'Add rule' button with a plus icon and an 'Apply' button. The 'Category' field is marked with an asterisk and has a dropdown menu with the text 'Select Tag Category'. The 'Value' field is also marked with an asterisk and has a text input area with the placeholder 'Enter the tag value to be applied'. Below these fields is a 'Description' section with a text area containing the placeholder 'Describe the purpose and application of this tag rule'. At the bottom right of the dialog, there are 'Cancel' and 'Save Tag' buttons.

## Create New Tag

**Dynamic** **Static**

**Tag rule**

☒ Match All ☐ Match Any

Search by typing a valid query

Add Filter +

+ Add rule Apply

\* **Category**

Select Tag Category

\* **Value**

Enter the tag value to be applied

**Description**

Describe the purpose and application of this tag rule

× Cancel Save Tag

3. Select the tag type you want to create:

**Tip:** For more information, see [Tag Format and Application](#).

- **Dynamic** – Tenable Exposure Management automatically applies the tag to the assets on your instance that match the tag rules.

The **Tag Rule** section appears:



**Note:** Tag rules must include valid queries and filters for the dynamic tag to function as expected.

- a. In the **Tag Rule** section, select how to apply the tag rule:
- **Match All** – If an asset matches every individual filter defined within the rule, Tenable Exposure Management.
  - **Match Any** – If an asset matches one or more of the filters defined in the tag rule, Tenable Exposure Management applies the tag to that asset.
- b. In the query text box, type the query you want to use to filter the assets to which the tag applies.

**Tip:** This query text box works the same as the [Global Asset Search](#).

To the right of the **Create New Tag** options, an asset list appears filtered by your query.

### Create New Tag

Dynamic

Static

Tag rule

☒ Match All

☐ Match Any

AS

Device

×

Add Filter +

⊕ Add rule

Apply

\* Category

Select Tag Category

\* Value

Enter the tag value to be applied

Description

Describe the purpose and application of this tag rule

1,423 assets included

1,423 assets included

Asset Name	Sources	Asset Class	AES	Active Finding Count	Top Attack Paths	Associated Ta...	Last
backup	🔍	📁 Device	🔴 945	62	107	42	25 A
target2	🔍	📁 Device	🔴 944	53	46	28	25 A
dcl	🔍	📁 Device	🔴 940	39	0	33	20 A
adcom1	🔍	📁 Device	🔴 892	81	123	25	25 A
tenable-ad-sen	🔍	📁 Device	🔴 891	145	0	32	6 Au
exchl	🔍	📁 Device	🔴 891	68	103	24	25 A
sql1	🔍	📁 Device	🔴 838	580	303	27	25 A
scom	🔍	📁 Device	🔴 835	431	185	20	25 A
sql2014	🔍	📁 Device	🔴 835	420	184	22	25 A
vcenterui2	🔍	📁 Device	🔴 835	415	183	23	25 A
adstarget	🔍	📁 Device	🔴 835	427	185	19	25 A
win-shlr183int0	🔍	📁 Device	🔴 835	361	171	20	25 A
windows2012	🔍	📁 Device	🔴 835	384	179	20	25 A
tenable-ad-sql	🔍	📁 Device	🔴 834	50	107	25	25 A

- c. (Optional) To further filter the list of assets to which the tag applies, click **Add Filter<sup>+</sup>**:



- i. Do one of the following:
  - To add a filter based on tags, click **Tags**.
  - To add a filter based on asset property, click **Properties**.
- ii. In the **Tag** or **Properties** list, select the tag or property for which you want to add a rule.

A logic operator window appears.

- iii. Select one of the following operators:

Operator	Description
<b>include tag</b>	Filters for items that include the selected tag.
<b>exclude tag</b>	Filters for items that exclude the selected tag.
<b>is equal to / includes / include property</b>	Filters for items that include the filter value.
<b>is not equal to / excludes / exclude property</b>	Filters for items that do not include the filter value.
<b>is greater than</b>	Filters for items greater than the filter value.
<b>is less than</b>	Filters for items less than the filter value.
<b>matches</b>	Filters for items that match the filter value.
<b>does not match</b>	Filters for items that do not match the filter value.



Operator	Description
<b>contains</b>	Filters for items that contain the filter value.
<b>does not have</b>	Filters for items that do not contain the filter value.
<b>has only</b>	Filters for items that have only the filter value.

**Note:** The available operators depend on your selection from the **Tag** or **Properties** list.

- iv. Where applicable, in the text box, type the constraint value to use for the filter.

**Tip:** Some text filters support the character (\*) as a wildcard to stand in for a section of text in the filter value. For example, if you want the filter to include all values that end in 1, type \*1. If you want the filter to include all values that begin with 1, type 1\*.

You can also use the wildcard operator to filter for values that contains certain text. For example, if you want the filter to include all values with a 1 somewhere between the first and last characters, type \*1\*.

- v. Click **Apply**.

Tenable Exposure Management applies the filter to the tag rule.

- **Static – You must manually apply the tag to individual assets.**

To the right of the **Create New Tag** options, an asset list appears.



^ Include Assets (Optional)

Selection Mode

Select a mode to include the assets to the current tag, either select assets one by one, or create a query that will return every assets that match the filters you choose to apply

Manual Selection

Batch

Q Search

Filter ▾

	Name	AES ▾		Type	Category
<input type="checkbox"/>	dc1	<div><div></div></div>	916	HOST	<div><div></div></div>
<input type="checkbox"/>	sql1	<div><div></div></div>	892	HOST	<div><div></div></div>
<input type="checkbox"/>	tenable-ad-sql	<div><div></div></div>	877	HOST	<div><div></div></div>
<input type="checkbox"/>	adcon1	<div><div></div></div>	870	HOST	<div><div></div></div>
<input type="checkbox"/>	adfs1	<div><div></div></div>	860	HOST	<div><div></div></div>
<input type="checkbox"/>	allow_honeymoon_sg-0262aac0d1c1b7344	<div><div></div></div>	784	CLOUD_RESOU...	<div><div></div></div>
<input type="checkbox"/>	allow_honeymoon_sg-012bea8e8d8a35c3d	<div><div></div></div>	784	CLOUD_RESOU...	<div><div></div></div>
<input type="checkbox"/>	backup	<div><div></div></div>	760	HOST	<div><div></div></div>

a. (Optional) Filter the asset list:

i. Click **Filter** ▾.

The **Add filter** + button appears.

ii. Click **Add filter** +.

A menu appears.

iii. Do one of the following:

◦ To search the asset list by tag, click **Tags**.

◦ To search the asset list by asset property, click **Properties**.

iv. In the search box, type the criteria by which you want to search the asset list.

Tenable Exposure Management populates a list of options based on your criteria.

v. Click the tag or property by which you want to filter the asset list.

A menu appears.



vi. Select how to apply the filter. For example, if you want to search for an asset whose name is *Asset14*, then select the **contains** radio button and in the text box, type *Asset14*.

vii. Click **Add filter**.

The filter appears above the asset list.

viii. Repeat these steps for each additional filter you want to apply.

ix. Click **Apply filters**.

Tenable Exposure Management filters the asset list by the designated criteria.

b. Select the check box next to the asset or assets to which you want to apply the tag.

4. In the **Category** box, do one of the following:

- Select an existing category to which to add the new tag.
- Add a new tag category:
  - a. In the text box, type a name for the new category.
  - b. At the bottom of the **Available Categories** drop-down, click **(New Category)**.

Tenable Exposure Management adds the new category.

5. In the **Value** text box, type a name for the tag value.

6. (Optional) In the Description text box, type a brief description of the tag.

7. Click **Save Tag**.

Tenable Exposure Management saves the tag and applies it to the appropriate assets. It may take several minutes to apply the tag to the selected assets and update any associated asset counts.

## Edit an Existing Tag

In the view, you can edit one or more components of a tag, including the category to which the tag belongs as well as the tag's name, description, and any rules applied to the tag.





**Note:** You can only edit tags created within Tenable Exposure Management.

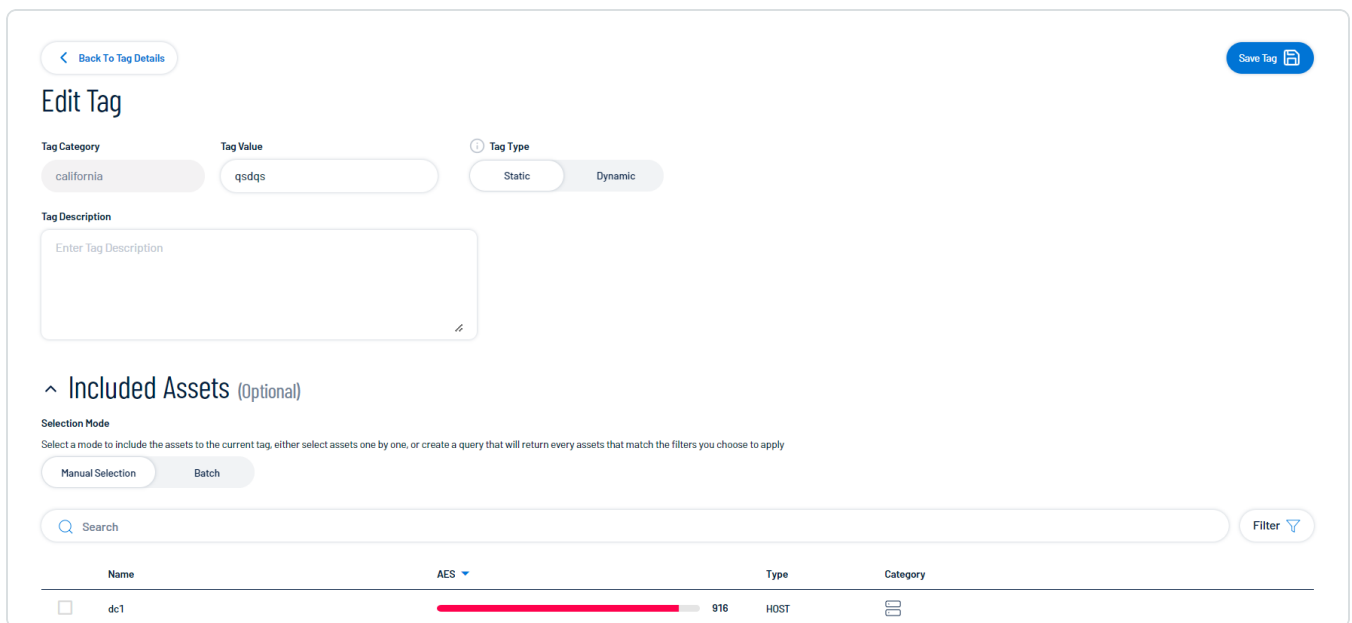
To edit a tag:

1. Access the [Tags](#) page.
2. In the tag list, in the row for the tag value or tag category you want to edit, click **See Details**.

The tag details page appears.

3. In the upper-right corner, click **Edit** .

The **Edit Tag** page appears.



[Back To Tag Details](#) **Save Tag**

### Edit Tag

Tag Category:  Tag Value:  Tag Type: ☒ Static ☐ Dynamic

Tag Description:


^ Included Assets (Optional)

Selection Mode:

Select a mode to include the assets to the current tag, either select assets one by one, or create a query that will return every assets that match the filters you choose to apply

[Filter](#)

Name	AES	Type	Category
<input type="checkbox"/> dc1	<div><div></div></div>	916	HOST

4. Make any desired changes.
5. Click **Save Tag** .

Tenable Exposure Management saves your changes to the tag value or tag category.

## Delete a Tag

In Tenable Exposure Management, you can delete the following components of a tag:



- Tag value — Tenable Exposure Management removes that specific tag from all assets where you applied the tag.



- Tag category – Tenable Exposure Management deletes any tags created under that category and removes those tags from all assets where you applied the tag.

**Note:** You can only delete tag values or tag categories created within Tenable Exposure Management.

To delete a tag:

1. Access the [Tags](#) page.
2. Do one of the following:
  - Delete one or more tag values or categories via the tag list:
    - a. Select the check box next to the tag that you want to delete.
    - b. At the top of the table, click **Remove** .
  - Delete a tag value or category via the tag details page:
    - a. In the tag list, in the row for the tag value or category you want to delete, click **See Details**.  
The tag details page appears.
    - b. In the upper-right corner, click **Delete** .

A confirmation message appears.

3. Click **Delete tags** .

Tenable Exposure Management does the following:

- If you deleted a tag value, Tenable Exposure Management deletes the tag value and removes it from all assets where you applied the tag.
- If you deleted a tag category, Tenable Exposure Management deletes the category, any tags created under that category, and removes those tags from all assets where you applied the tag.



## Connectors

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

### What is a Connector

Tenable Exposure Management ingests data from existing security tools, such as vulnerability scanners, cloud providers, inventory tools, SCA/SAST/DAST, and more. Connectors are how Tenable Exposure Management syncs and integrates with those tools and third-party data.

When successfully configuring an integration, Tenable Exposure Management syncs with the tool and the relevant data is ingested into Tenable Exposure Management.

Third party connectors in Tenable Exposure Management allow you to ingest data from applications outside of Tenable (third-party data) and display it alongside your Tenable product data in one seamless interface.

**Tip:** For information on connector Best Practices and FAQs, see the [Tenable Exposure Management Third-Party Connectors Quick Reference Guide](#).

### Why Integrate

The connectors integrate with the vendor tool to pull and ingest assets and vulnerability data into Tenable Exposure Management. Once the integration is complete, the platform analyzes the data to correlate, consolidate, and contextualize the ingested data to impact risk and remediation priority.

**Important:** When using Tenable Exposure Management connectors, Tenable recommends allowlisting the [IP addresses for the region](#) in which the Tenable Vulnerability Management site resides.

### Supported Integrations (Connectors)

Supported integrations include a variety of security tools and asset inventory from various vendors. Such security tools are:

- DAST
- CSPM



- CWPP
- IoT
- Network Scanners
- Endpoint Security
- Bug Bounty
- ASM
- Asset Inventory

Over time, Tenable will continue to add connectors to the **Connectors Library** in Exposure Management.

For the complete list of supported integrations, see [Supported Third-Party Integrations](#)

## Ingested Data

Exposure Management ingests assets, vulnerabilities (weaknesses), and findings from third-party vendors.

- [Assets](#): An asset is any object that represents a part of your organization's attack surface. Third party assets are defined as hosts, code projects, images, websites, or cloud resources ingested from a non-Tenable source.

For a complete list of ingested asset types, see [Asset Classes](#).

- [Weaknesses](#): Weaknesses are vulnerabilities and misconfigurations on your assets.
- [Findings](#): A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.

**Important!** On connector creation, it can take up to one hour for connector data to appear within Tenable Exposure Management.

## View and Manage your Connectors

To view your connectors:



1. In the left navigation menu, click **Connectors**.























Here you can see a list of your configured connectors.

Connectors

Add new connector

Search Connector Name

Select

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

Here you can:

- [Manage your connectors](#).
- Use the **Search** text box to search the list for a specific connector.
- Use the drop-down box to select a **Status** by which to filter the connectors page.

**Tip:** For more information, see [Connector Data Status](#).

## Connector Data Status

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

When you add and manage connectors in Exposure Management, each connector has a status that indicates its current state. These statuses help you understand where a connector is in its lifecycle and whether any action is needed.

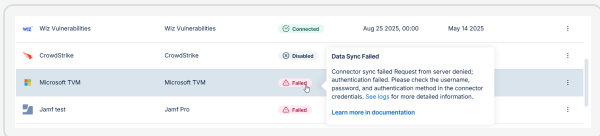
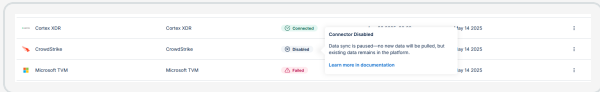


Connectors					<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Status"/>			
Name	Connector type	Data Status	Last data ingestion	Created on	
Rapid7	Rapid7	Failed	Jul 04 2023, 00:01	May 14 2025	
Cortex XDR	Cortex XDR	Connected	Aug 25 2025, 00:01	May 14 2025	
Rapid7 InsightVM Cloud	Rapid7 InsightVM Cloud	Connecting	Aug 25 2025, 00:02	May 14 2025	
Microsoft TVM - Davies	Microsoft TVM	Disabled	-	May 14 2025	
Armis test	Armis	Disabled	-	May 14 2025	
Wiz Cloud Configurations	Wiz Cloud Configurations	Connected	Aug 25 2025, 00:00	May 14 2025	
SHAY Wiz Issues	Wiz Issues	Failed	Aug 24 2025, 00:03	May 14 2025	
AWS Inspector V2	AWS Inspector V2	Connected	Aug 25 2025, 00:00	May 14 2025	
CrowdStrike TM	CrowdStrike	Disabled	-	May 13 2025	
Outpost24	Outpost24	Failed	Aug 24 2025, 00:00	May 13 2025	
WhiteHat Dast	WhiteHat Dast	Connected	Aug 25 2025, 00:01	May 13 2025	

The **Data Status** column in the **Connectors** page shows the latest state of the connector's data sync. Below is a description of each status you may encounter.

Status	Description	Recommended Action
Connecting	The connector is being configured and is not yet active. This is the initial status shown when you set up a new connector. It appears only during the initial setup while the platform is establishing a connection and performing the first data sync.	Wait for the sync to complete and for the status to change. No action is required unless the status does not change or the sync fails.
Connected	The connector is active and syncing	No action is needed. The connector is working as intended.



	data as expected. This status appears once the sync is successfully completed and data is imported into Exposure Management.	
Failed	Something went wrong during the sync process. If there is an issue with syncing data, the status will change to <b>Failed</b> .	<p>Click on the status to view the error description and access the logs.</p> 
Disabled	You can <a href="#">manually disable</a> a connector when you no longer want it to fetch new data. When disabled, the connector has stopped syncing, but existing data remains in the system.	<p>Click on the status to view the error description. You can re-enable the connector at any time to resume syncing. No data is lost during this state.</p> 
Blocked	The connector is blocked and data syncs are stopped due to a license limit.	Adjust or upgrade your plan to restore functionality.
Deleting	Exposure Management is removing the connector and its associated data. This status appears when	Wait for the process to complete. Once deletion is complete, the connector will no longer appear in the list.



you choose to delete a connector.

## What happens when you delete a connector?

When you [delete a connector](#), the connector row appears grayed out to indicate that the deletion process has started. Exposure Management removes the connector and its associated data.

Wait for the process to complete. Once deletion is complete, the connector will no longer appear in the list.

Name	Connector type	Data Status	Last data ingestion	Created on ↓	
Microsoft TVM	Microsoft TVM	Failed	Jun 10 2025, 00:04	May 14 2025	
Wiz Vulnerabilities	Wiz Vulnerabilities	Connected	Aug 26 2025, 00:01	May 14 2025	
RedHat Insights	RedHat Insights	Failed	Aug 12 2025, 00:01	May 14 2025	
Rapid7	Rapid7	Failed	Jun 04 2025, 00:01	May 14 2025	
Rapid7 InsightVM Cloud	Rapid7 InsightVM Cloud	Connected	Aug 26 2025, 00:01	May 14 2025	
Jamf test	Jamf Pro	Failed	-	May 14 2025	Deleting...
Microsoft TVM - Davies	Microsoft TVM	Disabled	-	May 14 2025	
Armist test	Armist	Disabled	-	May 14 2025	
Wiz Cloud Configurations	Wiz Cloud Configurations	Connected	Aug 26 2025, 00:03	May 14 2025	
Wiz Issues test	Wiz Issues	Failed	Aug 24 2025, 00:03	May 14 2025	

**Note:** To deep dive into status and sync logs, see [Connector Logs](#).

## Connector Logs

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

Tenable Exposure Management allows you to connect with third-party tools through connectors. To ensure visibility into sync operations, the platform includes a detailed Sync Log for each connector.

The **Connector Logs** in Tenable Exposure Management provide detailed insights into the processing lifecycle of your connectors.

You can use it to:



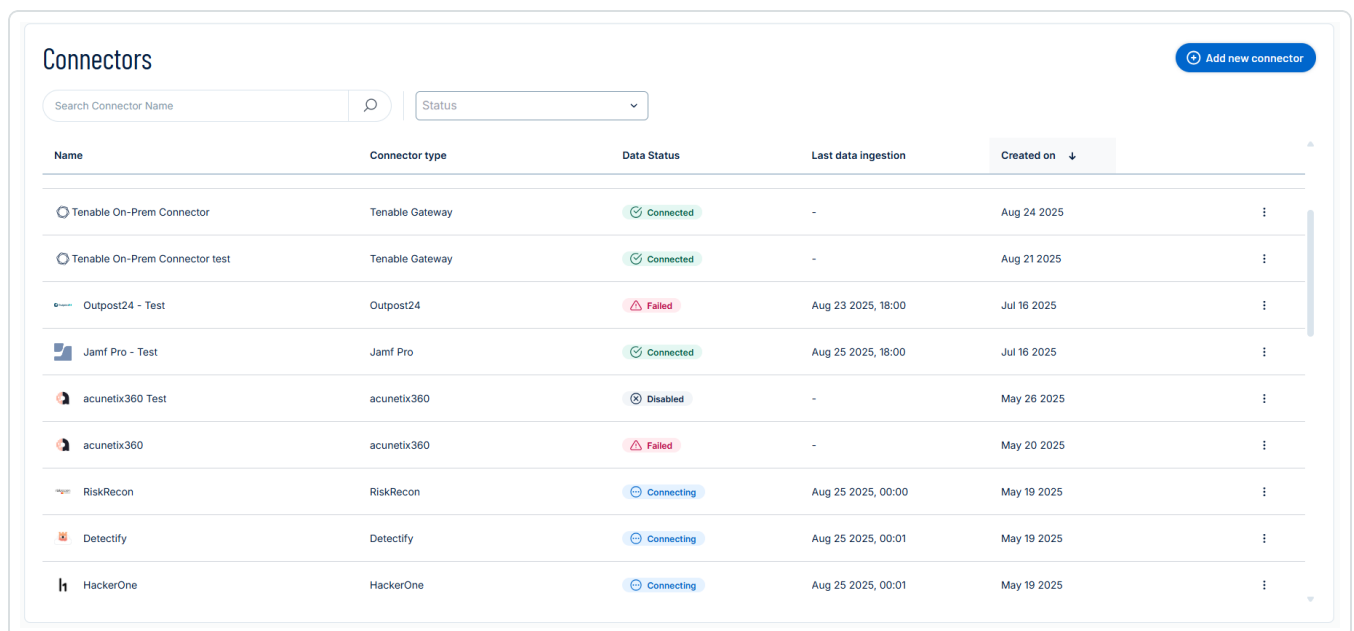


- Track sync history and progress
- Understand sync stages and timing
- Identify failed syncs and troubleshoot issues
- Filter log entries by Activity type, Data Stage, or Log Level.

## Access Connector Logs

To view connector's logs:

1. Navigate to the [Connectors](#) page.



The screenshot shows the 'Connectors' page in a web application. At the top right is a blue button labeled 'Add new connector'. Below the header is a search bar with the placeholder 'Search Connector Name' and a magnifying glass icon, followed by a 'Status' dropdown menu. The main content is a table with the following columns: 'Name', 'Connector type', 'Data Status', 'Last data ingestion', and 'Created on' (with a downward arrow). The table lists several connectors, including 'Tenable On-Prem Connector' (Connected), 'Tenable On-Prem Connector test' (Connected), 'Outpost24 - Test' (Failed), 'Jamf Pro - Test' (Connected), 'acunetix360 Test' (Disabled), 'acunetix360' (Failed), 'RiskRecon' (Connecting), 'Detectify' (Connecting), and 'HackerOne' (Connecting). Each row has a three-dot menu icon on the right side.

Name	Connector type	Data Status	Last data ingestion	Created on ↓
Tenable On-Prem Connector	Tenable Gateway	Connected	-	Aug 24 2025
Tenable On-Prem Connector test	Tenable Gateway	Connected	-	Aug 21 2025
Outpost24 - Test	Outpost24	Failed	Aug 23 2025, 18:00	Jul 16 2025
Jamf Pro - Test	Jamf Pro	Connected	Aug 25 2025, 18:00	Jul 16 2025
acunetix360 Test	acunetix360	Disabled	-	May 26 2025
acunetix360	acunetix360	Failed	-	May 20 2025
RiskRecon	RiskRecon	Connecting	Aug 25 2025, 00:00	May 19 2025
Detectify	Detectify	Connecting	Aug 25 2025, 00:01	May 19 2025
HackerOne	HackerOne	Connecting	Aug 25 2025, 00:01	May 19 2025

2. In the table, for the connector for which you want to view logs, click the **⋮** button.

A menu appears.

3. In the menu, click **Connector Logs**.

The connector sync logs appear in a clear, user-friendly table. Each sync cycle is listed



separately, allowing you to distinguish between different sync attempts.

Activity






▼

Data Stage

▼

Log Level

▼

	Start	End	Duration	Activity	Data Stage
>	Apr 15, 2025, 12:02 AM	Apr 15, 2025, 12:43 AM	40m 43s	Full Sync	 Failed
>	Apr 09, 2025, 12:03 AM	Apr 09, 2025, 1:06 AM	1h 2m	Incremental Sync	 Done
>	Apr 08, 2025, 12:03 AM	Apr 08, 2025, 12:48 AM	44m 55s	Incremental Sync	 In progress
>	Apr 07, 2025, 12:02 AM	Apr 07, 2025, 1:13 AM	1h 11m	Incremental Sync	 In progress
>	Apr 06, 2025, 12:03 AM	Apr 06, 2025, 12:52 AM	49m 27s	Incremental Sync	 In progress

## Reading Connector Logs

Select a sync row to expand it and view detailed information for troubleshooting. When a sync fails, the error message appears at the top of the expanded log with guidance on resolving the issue. You can also expand the full error payload to view the associated status code and headers.

Start	End	Duration	Activity	Data Stage	
▼	Aug 25 2025, 00:00	Aug 25 2025, 00:00	0m 4s	Full Sync	<span>⊗ Failed</span>

⊗ **Connector sync failed:** Connector sync failed Request from server denied; authentication failed. Please check the username, password, and authentication method in the connector credentials.

**Timestamp**  
Aug 25 2025, 00:00 ⊗ Connector sync failed Request from server denied; authentication failed. Please check the username, password, and authentication method in the connector credentials.  

Error Message ▼

{'status\_code': 401, 'headers': {'Cache-Control': 'no-store, no-cache', 'Pragma': 'no-cache', 'Content-Type': 'application/json; charset=utf-8', 'Expires': '-1', 'Strict-Transport-Security': 'max-age=31536000; includeSubDomains', 'X-Content-Type-Options': 'nosniff', 'P3P': 'CP="DSP CUR OTPI IND OTRI ONL FIN"', 'x-ms-request-id': 'd4635735-2522-4058-91a1-7a8d82f94e00', 'x-ms-ests-server': '2.1.21665.5 - SCUS ProdSlices', 'x-ms-srs': '1.P', 'Content-Security-Policy-Report-Only': 'object-src 'none'; base-uri 'self'; script-src 'self' 'nonce-BMe6yme3\_5ZyD7\_fmzndfA' 'unsafe-inline' 'unsafe-eval' https://\*.msauth.net https://\*.msftauth.net https://\*.msftauthimages.net https://\*.msauthimages.net https://\*.msidentity.com https://\*.microsoftonline-p.com https://\*.microsoftazuread-sso.com https://\*.azureedge.net https://\*.outlook.com https://\*.office.com https://\*.office365.com

**Data Lifecycle**

- ✓ **Initiating** 0m 3s
- ⊗ **Connectivity Test** 0m 0s
- 3 **Fetching** -
- 4 **Normalizing** -
- 5 **Processing** -

The expanded view includes:



- A readable error message with recommended actions
- A breakdown of the **Data Lifecycle** stages (Initiating, Connectivity Test, Fetching, Normalizing, and Processing)
- A full timestamp and error message block, including the root cause, error code (e.g., 'status\_code: 401'), and technical details
- A copy button for sharing or reporting error content
- Each log entry includes the sync start and end time, activity type, status, and durations for data ingestion and processing.

**Note:** The connector logs table retains sync data for 14 days, providing extended visibility into recent sync activity.

## Log Time Stamp




Log timestamps use your local browser time zone to ensure alignment with your environment.

	Start	End	Duration	Activity	Data Stage
▼	Aug 25 2025, 18:00	Aug 25 2025, 18:28	27m 48s	Full Sync	✓ Done
<div><div>Timestamp</div><div><div>Aug 25 2025, 18:28</div><div>Completed Processing</div></div><div><div>Aug 25 2025, 18:15</div><div>Started Processing</div></div><div><div>Aug 25 2025, 18:13</div><div>Completed Consolidation</div></div><div><div>Aug 25 2025, 18:10</div><div>Started Consolidation</div></div><div><div>Aug 25 2025, 18:08</div><div>Completed Normalizing Data</div></div></div>					

## Activity (Sync) Type

Tenable Exposure Management's data synchronization process with vendor connectors can be categorized into two distinct types: **Full Sync** and **Incremental Sync**.






Start	End	Duration	Activity	Data Stage
>  Apr 15, 2025, 12:02 AM	Apr 15, 2025, 12:43 AM	40m 43s	Full Sync	 Failed
> Apr 09, 2025, 12:03 AM	Apr 09, 2025, 1:06 AM	1h 2m	Incremental Sync	 Done

- **Full Sync:** A Full Sync pulls all available data from the vendor's system and ingests it into Exposure Management. This ensures that the platform has a complete, up-to-date view of the data supported by the connector.
- **Incremental Sync:** An Incremental Sync retrieves only new or changed records since the last successful sync. This method is used with connectors that support segmented or delta-based data retrieval, improving performance and reducing API consumption.

## Data Stage (Sync Status)

Each connector sync is assigned a high-level status.

This status appears in the Connector's log.

Start	End	Duration	Activity	Data Stage
> Apr 15, 2025, 12:02 AM	Apr 15, 2025, 12:43 AM	40m 43s	Full Sync	 Failed
> Apr 09, 2025, 12:03 AM	Apr 09, 2025, 1:06 AM	1h 2m	Incremental Sync	 Done
> Apr 08, 2025, 12:03 AM	Apr 08, 2025, 12:48 AM	44m 55s	Incremental Sync	 In progress

Data Stage	Description	Notes
Done	<ul style="list-style-type: none"><li>• The sync completed successfully.</li><li>• All lifecycle stages ran to completion without errors.</li><li>• Data is now updated and visible in Inventory, Weaknesses, and Analytics.</li></ul>	You can confirm data was successfully ingested and reflected.



<b>In Progress</b>	<ul style="list-style-type: none"><li>• The sync is currently running.</li><li>• One or more stages (e.g., Fetching, Normalization, or Processing) is still active.</li><li>• The log updates in real time as the sync progresses.</li></ul>	Check logs live to monitor what stage the sync is currently in and how long it's taking.
<b>Failed</b>	<ul style="list-style-type: none"><li>• The sync did not complete successfully.</li><li>• One or more stages failed (most commonly Connectivity Test, Fetching, or Processing).</li><li>• Error details appear in the Sync Log entry, including: Error message, Timestamp, Affected stage, and root cause/suggestion for next step (if available)</li></ul>	Open the Sync Log and review the failed stage to troubleshoot.

## Data Lifecycle Stages

Each connector sync goes through a structured set of backend stages. These stages are visible when expanding a sync log, allowing you to understand what happens during each part of the sync and where failures may occur.

Start	End	Duration	Activity	Data Stage
▼ Aug 25 2025, 18:00	Aug 25 2025, 18:28	27m 48s	Full Sync	Done
<div><div>Timestamp</div><div><div>Aug 25 2025, 18:28</div><div>Completed Processing</div></div><div><div>Aug 25 2025, 18:15</div><div>Started Processing</div></div><div><div>Aug 25 2025, 18:13</div><div>Completed Consolidation</div></div><div><div>Aug 25 2025, 18:10</div><div>Started Consolidation</div></div><div><div>Aug 25 2025, 18:08</div><div>Completed Normalizing Data</div></div></div>				
<div><div>Data Lifecycle</div><div><div>✓ Initiating</div><div>0m 2s</div></div><div><div>✓ Connectivity Test</div><div>0m 1s</div></div><div><div>✓ Fetching</div><div>0m 1s</div></div><div><div>✓ Normalizing</div><div>7m 50s</div></div><div><div>✓ Processing</div><div>13m 6s</div></div></div>				

Stage	Description	Notes
<b>Initiating</b>	<ul style="list-style-type: none"><li>• Begins the sync process.</li></ul>	<b>Possible Failures:</b> Invalid credentials,



	<ul style="list-style-type: none"><li>• Validates sync configuration and prepares the connector for execution.</li><li>• Triggers a connectivity test (same logic as the manual connectivity check in the connector settings).</li><li>• Logs basic metadata (e.g., sync type, trigger source).</li></ul>	expired tokens, network/authorization errors.
<b>Connectivity Test</b>	<ul style="list-style-type: none"><li>• Confirms the platform can reach and authenticate with the vendor's API.</li><li>• Verifies endpoint availability and token validity.</li><li>• Stops the sync if the vendor system is unavailable or responds with an error (e.g., 403, 500).</li></ul>	<p>This step is critical for establishing trust before any data is pulled.</p> <p><b>Possible Failures:</b></p> <ul style="list-style-type: none"><li>• Request issues (missing vendor info/internal errors).</li><li>• Permission or credentials issues.</li><li>• Network or server errors on the vendor's side.</li></ul>
<b>Fetching</b>	<ul style="list-style-type: none"><li>• Calls the vendor's API to pull asset, vulnerability, or configuration data.</li><li>• The volume and duration of this step vary based on: API rate limits Data size Type of fetch (Full</li></ul>	<p>This is often the longest stage, especially for high-volume connectors (e.g., cloud or endpoint sources).</p> <p><b>Possible Failures:</b></p> <ul style="list-style-type: none"><li>• Invalid status codes, response headers, or formats.</li></ul>



	<p>vs. Incremental)</p> <ul style="list-style-type: none"><li>• Data is retrieved as raw JSON from the vendor system.</li></ul>	<ul style="list-style-type: none"><li>• Vendor's server or network issues.</li></ul>
<b>Normalizing</b>	<ul style="list-style-type: none"><li>• Transforms raw vendor data into Tenable's internal standard format.</li><li>• Applies translation logic to fields (e.g., IP, hostname, asset metadata, vulnerability schema).</li><li>• Discards malformed or unusable records.</li><li>• Tags records for traceability to original source and sync cycle.</li></ul>	<p>The purpose of this stage is to ensure consistency across all data sources for unified presentation in Inventory, Exposure View, and Analytics.</p> <p><b>Possible Failures:</b> Internal issues in syncing data.</p>
<b>Processing</b>	<p>Enriches the normalized data with:</p> <ul style="list-style-type: none"><li>• Deduplication logic</li><li>• Asset merging (if multiple sources report the same entity)</li><li>• Tag applications (e.g., host groups, source tags)</li><li>• Risk metadata attachment (e.g., Exposure Score calculation)</li></ul>	<p>This is the final staging layer before data becomes visible in the platform.</p> <p><b>Possible Failures:</b></p> <ul style="list-style-type: none"><li>• Internal processing issues.</li></ul>



Connects findings to asset records.

## Connector Error Messages

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The following table lists common connector error codes and their associated user-facing messages. The messages and recommended actions appear in the following locations:

- The [Data Status](#) tooltip when you click on the connector status **Failed**
- The [connector sync logs](#)
- The **Test Connectivity** results during connector setup

Example:

Start	End	Duration	Activity	Data Stage
Aug 25 2025, 00:00	Aug 25 2025, 00:00	0m 4s	Full Sync	<span>Failed</span>

**Connector sync failed:**

Connector sync failed Request from server denied; authentication failed. Please check the username, password, and authentication method in the connector credentials.

Timestamp

Aug 25 2025, 00:00 Connector sync failed Request from server denied; authentication failed. Please check the username, password, and authentication method in the connector credentials.

Error Message

```
{'status_code': 401, 'headers': {'Cache-Control': 'no-store, no-cache', 'Pragma': 'no-cache', 'Content-Type': 'application/json; charset=utf-8', 'Expires': '-1', 'Strict-Transport-Security': 'max-age=31536000; includeSubDomains', 'X-Content-Type-Options': 'nosniff', 'P3P': 'CP="DSP CUR OTPI IND OTRI ONL FIN"', 'x-ms-request-id': 'd4635735-2522-4058-91a1-7a8d82f94e00', 'x-ms-ests-server': '2.1.21665.5 - SCUS ProdSlices', 'x-ms-srs': '1.P', 'Content-Security-Policy-Report-Only': 'object-src 'none'; base-uri 'self'; script-src 'self' 'nonce-BMe6yme3.5ZyD7fmzndfA' 'unsafe-inline' 'unsafe-eval' https://*.msauth.net https://*.msftauth.net https://*.msftauthimages.net https://*.msauthimages.net https://*.msidentity.com https://*.microsoftonline-p.com https://*.microsoftazuread-sso.com https://*.azureadon.net https://*.outlook.com https://*.office.com https://*.office365.com'}}
```

**Data Lifecycle**

- ✓ **Initiating** 0m 3s
- ✗ **Connectivity Test** 0m 0s
- 3 **Fetching** -
- 4 **Normalizing** -
- 5 **Processing** -

Error Code	Message	Recommended Action
400	Request from server failed.	Check that all details in the connector credentials section are correct. If the issue persists, please contact support.
401	Request from server denied; authentication	Check the username, password, and authentication method in the connector





Error Code	Message	Recommended Action
	failed.	credentials.
403	Request from server denied; access denied.	Make sure the account used in the connector set-up has sufficient permissions.
404	Request from server failed.	Check that all details in the connector credentials section are correct. If the issue persists, please contact support.
408	Request from server failed; timed out.	Make sure the vendor service is available and try again later.
409	Request from server failed; conflict detected.	Verify that the connector is not syncing duplicated or conflicting resources.
426	Request from server failed; timed out.	Make sure the vendor service is available and try again later.
428	Request from server failed; timed out.	Make sure the vendor service is available and try again later.
429	Request from server failed due to too many requests.	Check the rate limits and try again later.
500	Connection to server failed.	Make sure the vendor service is available and try again later.
501	Connection to server failed; not supported.	Verify the API version and supported methods.
502	Connection to server failed.	Make sure the vendor service is available and try again later.
503	Connection to server failed.	Make sure the vendor service is available and try again later.
504	Connection to server	Make sure the vendor service is



Error Code	Message	Recommended Action
	timed out.	available and try again later.
505	Request from server failed; not supported.	Verify the API version compatibility. If the issue persists, contact support.
507	Request from server failed due to insufficient storage to process the request.	Try again. If the issue persists, contact support.
508	Request from server failed; detected a processing loop.	Try again. If the issue persists, contact support.
511	Request from server denied; authentication failed.	Check the username, password, and authentication method in the connector credentials.
GRAPHQL_VALIDATION_FAILED	Request from server failed.	If the issue persists, contact support.
BAD_USER_INPUT	Request from server failed.	If the issue persists, contact support.
UNAUTHENTICATED	Request from server failed.	Verify that all details in the connector credentials section are correct.
FORBIDDEN	Request from server failed.	Verify that all details in the connector credentials section are correct.
INTERNAL_SERVER_ERROR	Request from server failed.	If the issue persists, contact support.
PERSISTED_QUERY_NOT_FOUND	Request from server failed.	If the issue persists, contact support.
RATE_LIMITED	Request from server failed.	Check the rate limits and try to sync again later.



Error Code	Message	Recommended Action
SERVICE_UNAVAILABLE	Request from server failed.	Verify connectivity by testing the API endpoint directly (e.g., using CURL).
ENOTFOUND	Request from server failed.	Verify that all details in the connector credentials section are correct.
SSL_ERROR	Request from server failed.	Verify that all details in the connector credentials section are correct.
Not applicable	Internal Error	Our team has been notified and is working to resolve the issue. Your data will be processed with the next successful sync.

## Manage Connectors

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

In Tenable Exposure Management, you can manage your third party connectors in the following ways:

### Add a New Connector

Add a connector to ingest third party asset and finding data into Exposure Management.

To add a new connector:



1. Navigate to the [Connectors](#) page.

### Connectors

Status

Add new connector

Name	Connector type	Data Status	Last data ingestion	Created on	
Tenable On-Prem Connector	Tenable Gateway	Connected	-	Aug 24 2025	
Tenable On-Prem Connector test	Tenable Gateway	Connected	-	Aug 21 2025	
Outpost24 - Test	Outpost24	Failed	Aug 23 2025, 18:00	Jul 16 2025	
Jamf Pro - Test	Jamf Pro	Connected	Aug 25 2025, 18:00	Jul 16 2025	
acunetix360 Test	acunetix360	Disabled	-	May 26 2025	
acunetix360	acunetix360	Failed	-	May 20 2025	
RiskRecon	RiskRecon	Connecting	Aug 25 2025, 00:00	May 19 2025	
Detectify	Detectify	Connecting	Aug 25 2025, 00:01	May 19 2025	
HackerOne	HackerOne	Connecting	Aug 25 2025, 00:01	May 19 2025	

2. In the upper-right corner, click **+ Add new connector**.

The **Connectors Library** appears.

### Connector Library

#### Categories

ASM	1
Asset Inventory	4
Bug Bounty	1
CSPM	5
CWPP	3
DAST	8
EDR	8
OT	1
VM	12

acunetix360

DAST

Connect

Acunetix Premium

DAST

Connect

Aqua CWPP

CWPP

Connect

Armis

OT

Connect

AWS Config

EDR

Connect

AWS EC2

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

- 352 -



- On the tile for the connector, click **Connect**.

The connector configuration options appear.

- Configure the connector according to the specific connector's configuration instructions. For more information on connector types and how to configure them, see [Supported Third-Party Integrations](#).

## View Connector Status and Logs

The **Connector Logs** in Tenable Exposure Management provide detailed insights into the processing lifecycle of your connectors, including both the actual processing time and any waiting time that occurs when multiple connectors are syncing simultaneously.

To view your connector logs:

- Navigate to the [Connectors](#) page.

Connectors

Search Connector Name

Status

Add new connector

Name	Connector type	Data Status	Last data ingestion	Created on	
<div><div></div>Tenable On-Prem Connector</div>	Tenable Gateway	<div><div></div>Connected</div>	-	Aug 24 2025	<div></div>
<div><div></div>Tenable On-Prem Connector test</div>	Tenable Gateway	<div><div></div>Connected</div>	-	Aug 21 2025	<div></div>
<div><div></div>Outpost24 - Test</div>	Outpost24	<div><div></div>Failed</div>	Aug 23 2025, 18:00	Jul 16 2025	<div></div>
<div><div></div>Jamf Pro - Test</div>	Jamf Pro	<div><div></div>Connected</div>	Aug 25 2025, 18:00	Jul 16 2025	<div></div>
<div><div></div>acunetix360 Test</div>	acunetix360	<div><div></div>Disabled</div>	-	May 26 2025	<div></div>
<div><div></div>acunetix360</div>	acunetix360	<div><div></div>Failed</div>	-	May 20 2025	<div></div>
<div><div></div>RiskRecon</div>	RiskRecon	<div><div></div>Connecting</div>	Aug 25 2025, 00:00	May 19 2025	<div></div>
<div><div></div>Detectify</div>	Detectify	<div><div></div>Connecting</div>	Aug 25 2025, 00:01	May 19 2025	<div></div>
<div><div></div>HackerOne</div>	HackerOne	<div><div></div>Connecting</div>	Aug 25 2025, 00:01	May 19 2025	<div></div>

- In the table, for the connector for which you want to view logs, click the **:** button.

A menu appears.

- In the menu, click **Connector Logs**.

The connector sync logs appear in a clear, user-friendly table. Each sync cycle is listed separately, allowing you to distinguish between different sync attempts.



Activity		Data Stage		Log Level	
Start	End	Duration	Activity	Data Stage	
> Apr 15, 2025, 12:02 AM	Apr 15, 2025, 12:43 AM	40m 43s	Full Sync	Failed	
> Apr 09, 2025, 12:03 AM	Apr 09, 2025, 1:06 AM	1h 2m	Incremental Sync	Done	
> Apr 08, 2025, 12:03 AM	Apr 08, 2025, 12:48 AM	44m 55s	Incremental Sync	In progress	
> Apr 07, 2025, 12:02 AM	Apr 07, 2025, 1:13 AM	1h 11m	Incremental Sync	In progress	
> Apr 06, 2025, 12:03 AM	Apr 06, 2025, 12:52 AM	49m 27s	Incremental Sync	In progress	

4. **Tip:** You can also access the connector logs directly from the connector setup page.

The logs display sync history, timestamps, types (Full or Incremental), and error messages (if any).

## Schedule Connector Sync Time

Set connector sync schedules to keep data fresh, consistent, and aligned with your operational needs. Configure specific sync times and days to reduce system load, improve performance, and give your team timely access to accurate security data.

To schedule connector sync time:



1. Navigate to the [Connectors](#) page.

Connectors

Search Connector Name

Status

Add new connector

Name	Connector type	Data Status	Last data ingestion	Created on	
Tenable On-Prem Connector	Tenable Gateway	Connected	-	Aug 24 2025	
Tenable On-Prem Connector test	Tenable Gateway	Connected	-	Aug 21 2025	
Outpost24 - Test	Outpost24	Failed	Aug 23 2025, 18:00	Jul 16 2025	
Jamf Pro - Test	Jamf Pro	Connected	Aug 25 2025, 18:00	Jul 16 2025	
acunetix360 Test	acunetix360	Disabled	-	May 26 2025	
acunetix360	acunetix360	Failed	-	May 20 2025	
RiskRecon	RiskRecon	Connecting	Aug 25 2025, 00:00	May 19 2025	
Detectify	Detectify	Connecting	Aug 25 2025, 00:01	May 19 2025	
HackerOne	HackerOne	Connecting	Aug 25 2025, 00:01	May 19 2025	

2. In the table, click the connector for which you want to schedule the sync time.

The connector setup page appears.

3. In the [Connector Scheduling](#) section, configure the desired sync time.

## Edit Connector Settings

To edit connector settings:



1. Navigate to the [Connectors](#) page.

Connectors

Search Connector Name

Status

Add new connector

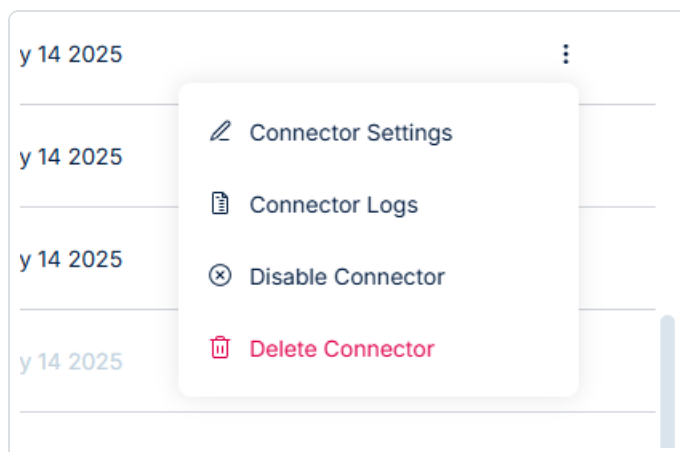
Name	Connector type	Data Status	Last data ingestion	Created on	
Tenable On-Prem Connector	Tenable Gateway	Connected	-	Aug 24 2025	
Tenable On-Prem Connector test	Tenable Gateway	Connected	-	Aug 21 2025	
Outpost24 - Test	Outpost24	Failed	Aug 23 2025, 18:00	Jul 16 2025	
Jamf Pro - Test	Jamf Pro	Connected	Aug 25 2025, 18:00	Jul 16 2025	
acunetix360 Test	acunetix360	Disabled	-	May 26 2025	
acunetix360	acunetix360	Failed	-	May 20 2025	
RiskRecon	RiskRecon	Connecting	Aug 25 2025, 00:00	May 19 2025	
Detectify	Detectify	Connecting	Aug 25 2025, 00:01	May 19 2025	
HackerOne	HackerOne	Connecting	Aug 25 2025, 00:01	May 19 2025	

2. In the table, locate the connector you want to edit.

3. To access the connector setup page, do one of the following:

- In the table, click the name of the connector you want to edit.
- In the table, next to the connector you want to edit, click the button.

A menu appears.



a. Click **Connector Settings**.

The connector setup page appears.





4. Update the connector settings based on your desired configuration options. Here, you can configure:

- Connector credentials
- Data pulling configuration
- Connector scheduling

**Tip:** For more information about specific connectors and how to configure them, see [Supported Third-Party Integrations](#).

5. Once complete, do one of the following:

- **Cancel** – Discard any changes.
- **Update and sync now** – Apply your changes and immediately trigger a full sync for the connector.
- **Update** – A confirmation message appears. Here, you can choose whether to apply the changes immediately or on the configured sync schedule.

### Edit CrowdStrike Connector

Editing the connector configuration will affect the ingested data. Are you sure you want to update the connector?

CancelUpdate and sync on configured timeUpdate and sync now

## Disable or Enable a Connector

You can manually disable a connector when you no longer want it to fetch new data.

To disable a connector:



1. Navigate to the [Connectors](#) page.

Connectors

Search Connector Name

Status

Add new connector

Name	Connector type	Data Status	Last data ingestion	Created on	
Tenable On-Prem Connector	Tenable Gateway	Connected	-	Aug 24 2025	
Tenable On-Prem Connector test	Tenable Gateway	Connected	-	Aug 21 2025	
Outpost24 - Test	Outpost24	Failed	Aug 23 2025, 18:00	Jul 16 2025	
Jamf Pro - Test	Jamf Pro	Connected	Aug 25 2025, 18:00	Jul 16 2025	
acunetix360 Test	acunetix360	Disabled	-	May 26 2025	
acunetix360	acunetix360	Failed	-	May 20 2025	
RiskRecon	RiskRecon	Connecting	Aug 25 2025, 00:00	May 19 2025	
Detectify	Detectify	Connecting	Aug 25 2025, 00:01	May 19 2025	
HackerOne	HackerOne	Connecting	Aug 25 2025, 00:01	May 19 2025	

2. In the table, next to the connector you want to disable, click the button.

A menu appears.

y 14 2025

Connector Settings

Connector Logs

Disable Connector

Delete Connector

3. Click **Disable Connector**.

Tenable Exposure Management updates the status of the connector to **Disabled**.

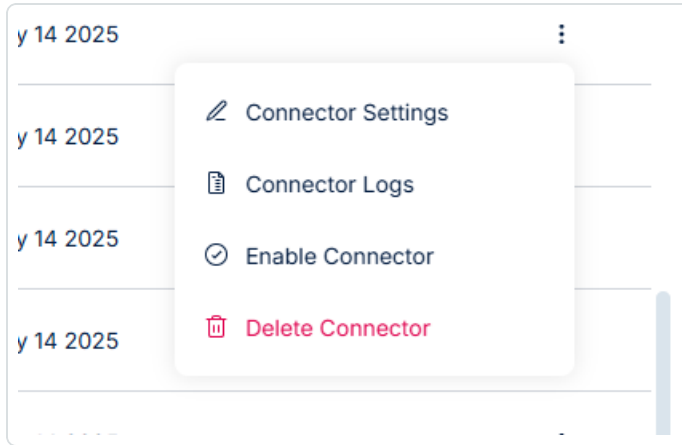
To resume syncing data for a disabled connector, you can re-enable the connector at any time. No data is lost during this state.

To enable a connector:



1. In the Connectors table, next to the connector you want to enable, click the  button.

A menu appears.



2. Click **Enable Connector**.

Tenable Exposure Management updates the status of the connector to **Enabled**.

## Delete a Connector

You can remove connectors and their associated data from Tenable Exposure Management.

**Important!** Full syncs can take up to 24 hours, at which point all connector data is fully removed from Tenable Exposure Management and its user interface.

To delete a connector:

1. Navigate to the [Connectors](#) page.

Connectors

Search Connector Name

Status

Add new connector

Name	Connector type	Data Status	Last data ingestion	Created on	
Tenable On-Prem Connector	Tenable Gateway	Connected	-	Aug 24 2025	
Tenable On-Prem Connector test	Tenable Gateway	Connected	-	Aug 21 2025	
Outpost24 - Test	Outpost24	Failed	Aug 23 2025, 18:00	Jul 16 2025	
Jamf Pro - Test	Jamf Pro	Connected	Aug 25 2025, 18:00	Jul 16 2025	
acunetix360 Test	acunetix360	Disabled	-	May 26 2025	
acunetix360	acunetix360	Failed	-	May 20 2025	
RiskRecon	RiskRecon	Connecting	Aug 25 2025, 00:00	May 19 2025	
Detectify	Detectify	Connecting	Aug 25 2025, 00:01	May 19 2025	
HackerOne	HackerOne	Connecting	Aug 25 2025, 00:01	May 19 2025	

2. In the table, next to the connector you want to delete, click the button.

A menu appears.

y 14 2025

Connector Settings

Connector Logs

Disable Connector

Delete Connector

3. Click **Delete Connector**.

The connector row appears grayed out to indicate that the deletion process has started.

Jamf test	Jamf Pro	Failed	-	May 14 2025	Deleting...
-----------	----------	--------	---	-------------	-------------



**Tip:** For more information about deleting connectors, tags, and their data, see [Deleted Connectors and Tags](#)

## Supported Third-Party Integrations

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

Tenable Exposure Management offers integration with the security tools listed in the table below.

Each supported integration has:

- Every supported integration has a dedicated **Connector** within Tenable Exposure Management with specific configurations.
- Each connector can belong to one or more security data sources.
- Some connectors support inventory only (ingest only assets data), while others support ingesting assets and vulnerability data.

**Tip:** To learn more, see [Connectors](#).

**Important!** On connector creation, it can take up to one hour for connector data to appear within Tenable Exposure Management.

## Security Tools Supported Integrations

The following connectors ingest both asset and weakness data.

Supported Integration	Connector Name and Documentation	Security Tool Category	Ingested Asset Classes
<a href="#">Acunetix360</a>	<a href="#">Acunetix360 Connector</a>	DAST	Web Application
<a href="#">Acunetix Premium</a>	<a href="#">Acunetix Premium Connector</a>	DAST	Web Application
<a href="#">Armis</a>	<a href="#">Armis Connector</a>	Operational Technology (OT)	Device



Supported Integration	Connector Name and Documentation	Security Tool Category	Ingested Asset Classes
<a href="#">AWS Inspector</a>	<a href="#">AWS Inspector Connector</a>	CSPM	Cloud Resource
<a href="#">BitSight</a>	<a href="#">BitSight Connector</a>	DAST	Device, Web Application
<a href="#">BlackDuck (formerly WhiteHat)</a>	<a href="#">BlackDuck (formerly WhiteHat) Connector</a>	DAST	Web Application
<a href="#">Cortex XDR</a>	<a href="#">Cortex XDR Connector</a>	Endpoint Security	Device
<a href="#">CrowdStrike</a>	<a href="#">CrowdStrike Connector</a>	Endpoint Security	Device
<a href="#">Cycognito</a>	<a href="#">Cycognito Connector</a>	DAST	Device, Web Application
<a href="#">Detectify</a>	<a href="#">Detectify Connector</a>	DAST	Web Application
<a href="#">Microsoft TVM</a>	<a href="#">Microsoft TVM Connector</a>	Endpoint Security	Device
<a href="#">Outpost 24</a>	<a href="#">Outpost 24 Connector</a>	Endpoint Security	Device, Web Application
<a href="#">PrismaCloud CWPP</a>	<a href="#">PrismaCloud CWPP Connector</a>	VM (CWPP)	Device, Container
<a href="#">Purplemet</a>	<a href="#">Purplemet Connector</a>	DAST	Web Application
<a href="#">Qualys</a>	<a href="#">Qualys Connector</a>	Endpoint Security	Device
<a href="#">Qualys WAS</a>	<a href="#">Qualys WAS Connector</a>	DAST	Web Application
<a href="#">Rapid7 Insight Appsec</a>	<a href="#">Rapid7 Insight AppSec</a>	DAST	Web Application



Supported Integration	Connector Name and Documentation	Security Tool Category	Ingested Asset Classes
	<a href="#">Connector</a>		
<a href="#">Rapid7 Insight VM</a>	<a href="#">Rapid7 Insight VM Connector</a>	Endpoint Security	Device
<a href="#">Rapid7 InsightVM Cloud</a>	<a href="#">Rapid7 Insight VM Cloud</a>	Endpoint Security	Device
<a href="#">Red Hat Insights</a>	<a href="#">Red Hat Insights Connector</a>	Endpoint Security	Device
<a href="#">RiskRecon</a>	<a href="#">RiskRecon Connector</a>	DAST	Web Application
<a href="#">SecurityScorecard</a>	<a href="#">SecurityScorecard Connector</a>	DAST	Web Application
<a href="#">SentinelOne</a>	<a href="#">SentinelOne Connector</a>	Endpoint Security	Device, Other
<a href="#">Tanium</a>	<a href="#">Tanium Connector</a>	Endpoint Security	Device
<a href="#">Veracode</a>	<a href="#">Veracode Connector</a>	DAST	Web Application
<a href="#">Wiz Vulnerabilities</a>	<a href="#">Wiz Vulnerabilities Connector</a>	CWPP (VM)	Device, Container, Resource, Other
<a href="#">Wiz Configurations</a>	<a href="#">Wiz Configurations Connector</a>	CSPM	Device, Container, Resource, Other
<a href="#">Wiz Issues</a>	<a href="#">Wiz Issues Connector</a>	ASM	Device, Container, Resource, Other

## Asset Inventory Supported Integrations

The following connectors ingest asset data only.

Supported	Connector Name and	Ingested Asset
-----------	--------------------	----------------



Integration	Documentation	Classes
<a href="#">AWS EC2</a>	<a href="#">AWS EC2 Connector</a>	Device
<a href="#">Axonius</a>	<a href="#">Axonius Connector</a>	Device
<a href="#">Microsoft Azure</a>	<a href="#">Azure Connector</a>	Device
<a href="#">Microsoft Intune</a>	<a href="#">Intune Connector</a>	Device
<a href="#">Jamf</a>	<a href="#">Jamf Pro Connector</a>	Device
<a href="#">ServiceNow</a>	<a href="#">ServiceNow Connector</a>	Device, Web Application

## Bug Bounty Supported Integrations

The following connectors ingest bug bounty data.

Supported Integration	Connector Name and Documentation	Ingested Asset Classes	Category
<a href="#">HackerOne</a>	<a href="#">HackerOne Connector</a>	Web Application	Bug Bounty

## Other Integrations

Supported Integration	Connector Name and Documentation	Category
Tenable On-Prem	<a href="#">Tenable On-Prem Connector</a>	On-Prem

## Acunetix360 Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Acunetix360](#) is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other





exploitable vulnerabilities. In general, Acunetix scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Acunetix360</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Generate an Acunetix360 User ID and Token:**
  1. Log in to your Acunetix 360 account.
  2. Click on your name in the top-right corner of the page and select API Settings from the drop down menu.
  3. If prompted, enter your current password and click **Submit**.



Your **User ID** and **API Token** appear.

**Tip:** For detailed instructions, refer to the [Acunetix 360 API Settings](#) documentation.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

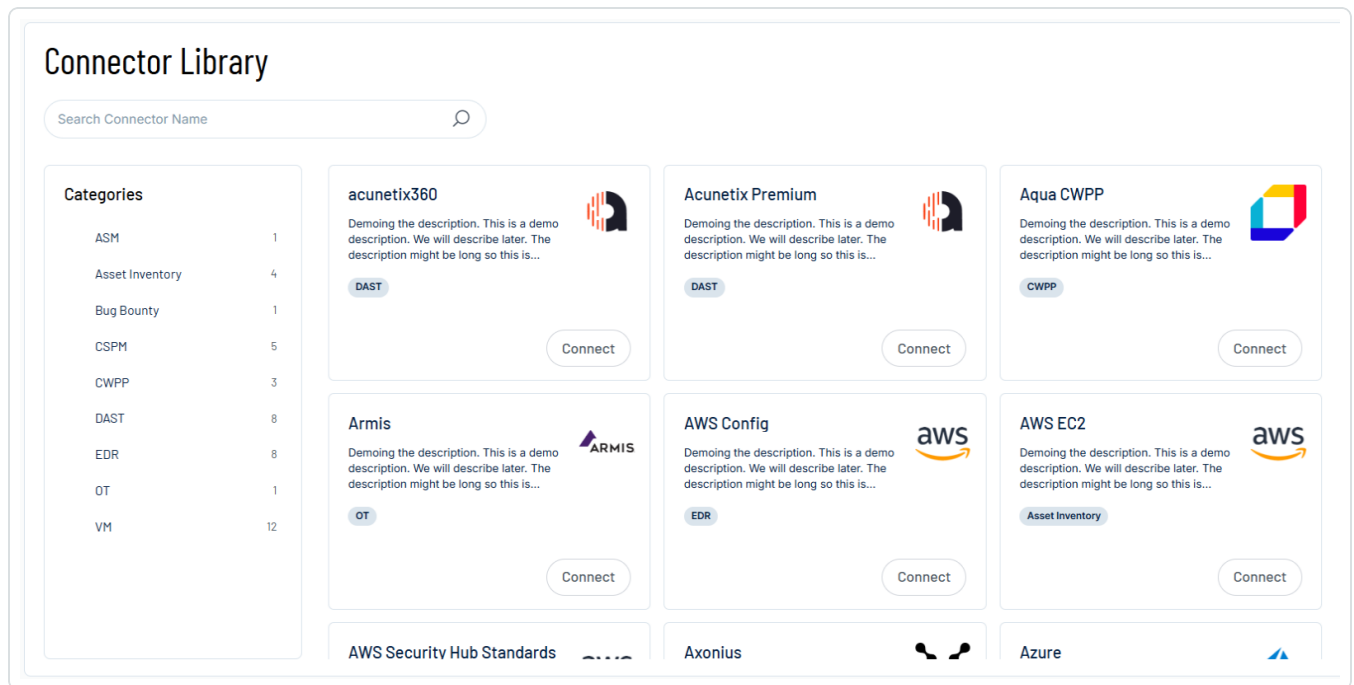
Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **User ID** and **API Token** text boxes, paste the credentials you generated in Acunetix360.
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.



- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.

- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

Show tests ▼

**Successful tests** 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.



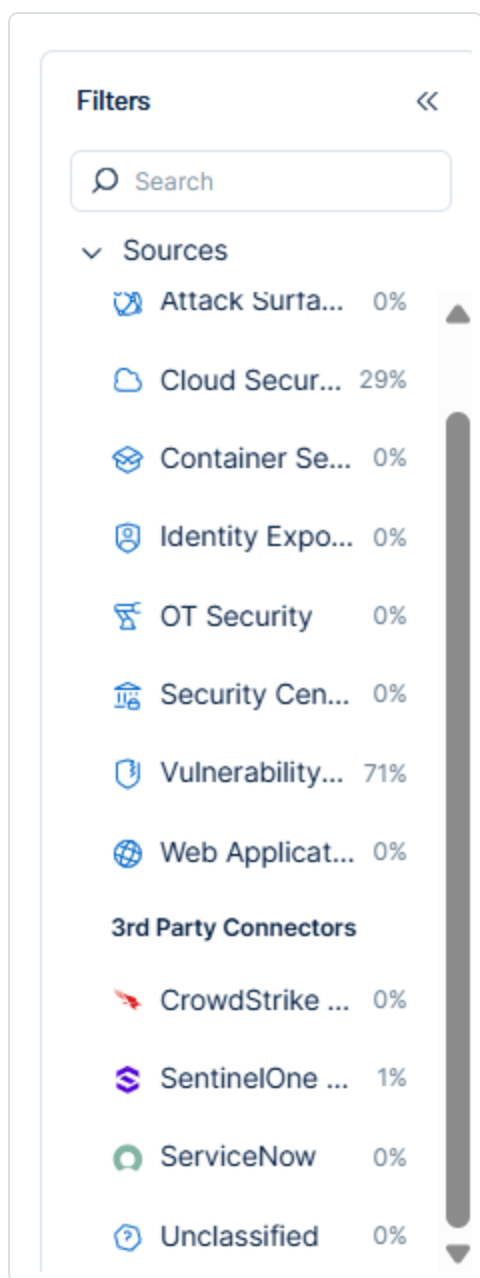
## Acunetix 360 in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

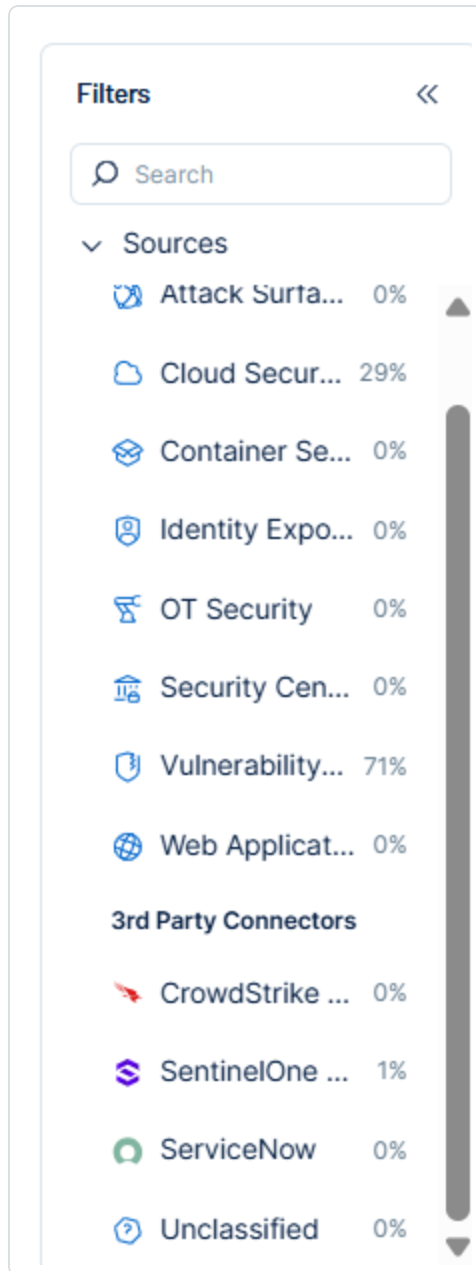
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

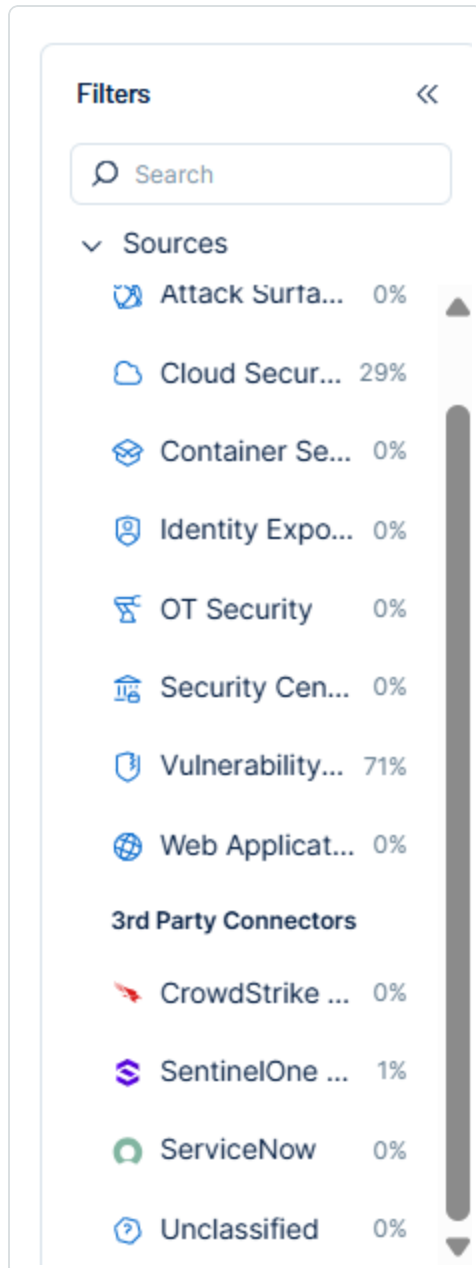
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings







The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management Value	Acunetix360 Value
Unique Identifier	Id
Asset - Name	Name
Asset - First Observation Date	CreatedAt
Asset - Last Observed At	UpdatedAt
Asset - Webapp Homepage Screenshot Url	RootUrl
Asset - External Tags	Tags
Asset Custom Attributes	Id Description TechnicalContactEmail Groups Name IsVerified LicenseType AgentMode

## Finding Mapping



Tenable Exposure Management UI Field	Acunetic360 Field
Unique Identifier	Id and Url
Finding Name	Title
CWEs	Classification.Cwe
Severity Driver	Severity
Description	Summary
First Seen	first_seen
Last seen (Observed)	last_seen
Finding Custom Attributes	url Description Actions External References Impact Proof Of Concept Skills Type CvssVectorString Cvss31VectorString Classification Cvss Score Cvss31 Score Order Severity

## Finding Status Mapping



Tenable Exposure Management Status	Acunetix360 Status
Active	All other statuses, including: Present , False Positive, and Accepted Risk
Fixed	Fixed

**Note:**For Acunetix360, Exposure Management uses the State field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	Acunetic360 Score
Critical	<b>Severity:</b> Critical
High	<b>Severity:</b> High
Medium	<b>Severity:</b> Medium
Low	<b>Severity:</b> Low

**Note:**For Acunetix360, Exposure Management uses the Severity field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a>
Change a Finding status from "Active" to "Fixed"	Finding status changes to State.split = Fixed on the vendor side



**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	Id
Finding	Id + Url

## API Endpoints in Use

API	Use in Tenable Exposure Management
<a href="https://online.acunetix360.com/api/1.0/websites/list">https://online.acunetix360.com/api/1.0/websites/list</a>	Assets (Web applications)
<a href="https://online.acunetix360.com/api/1.0/issues/allissues">https://online.acunetix360.com/api/1.0/issues/allissues</a>	Findings

## Acunetix Premium Cloud Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Acunetix Premium](#) is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, cross-site scripting, and other exploitable vulnerabilities. Acunetix scans any website or web application accessible via a web browser and uses the HTTP/HTTPS protocol.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).



## Connector Details

Details	Description
Supported products	<a href="#">Acunetix Premium</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Create an Acunetix Premium user with **Platform Administrator** permissions.
- Identify your Acunetix Premium server URL (e.g., <https://online.acunetix.com/api/v1>).
- **Generate an Acunetix Premium API Key:**
  1. Log in to your Acunetix Premium Cloud account at <https://online.acunetix.com>.
  2. Click on your username in the top-left corner of the dashboard.
  3. Select Profile from the dropdown menu.
  4. Scroll down to the **API Key** section.
  5. Click **Generate new API key**.
  6. Click **Show** to display your new API key, or **Copy** to copy it to your clipboard.



### API Key

Hidden for security reasons

Copy

Show

Generate New Api Key

Delete

[Acunetix API Documentation](#)

**Important!** Do not enable two-factor authentication. If enabled, the connector will not be able to access the data.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.























The **Connectors** page appears.

Connectors

Search Connector Name

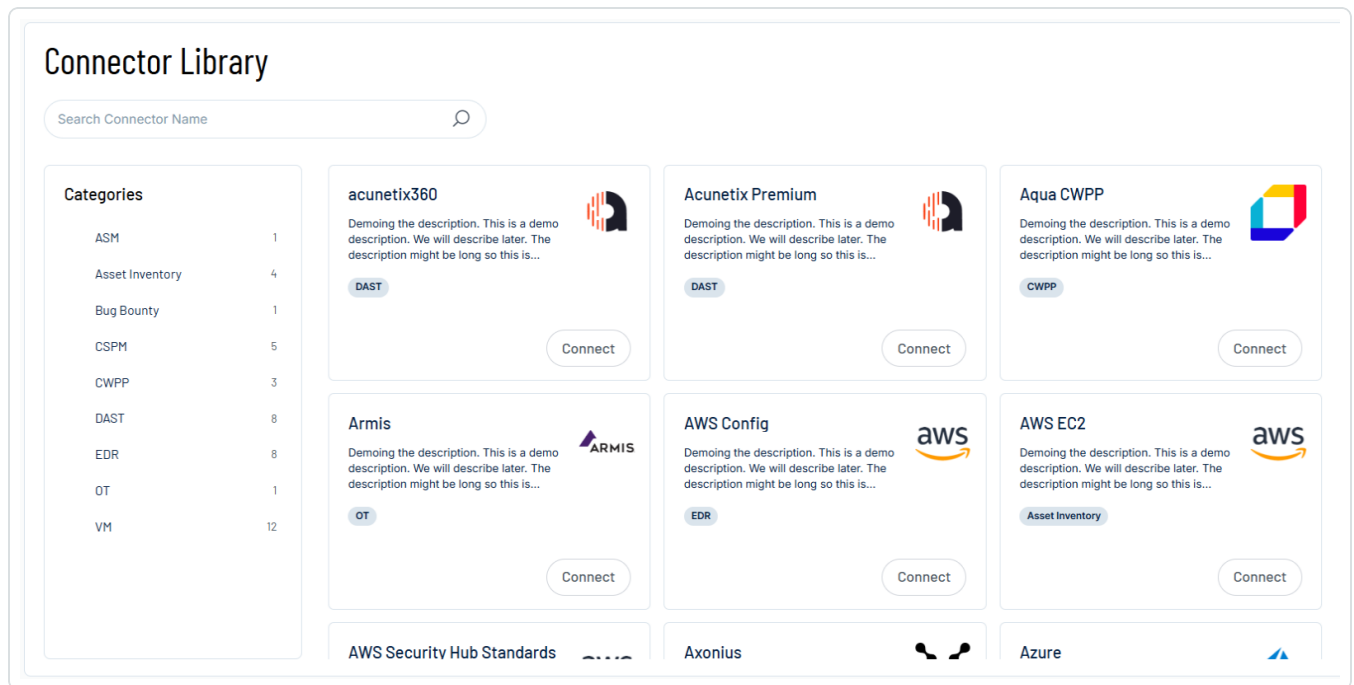
Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server Url** text box, type your Acunetix server UR: (https://online.acunetix.com/api/v1).
4. In the **API Key** text box, paste the API key you generated in Acunetix Premium.



5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:





- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.

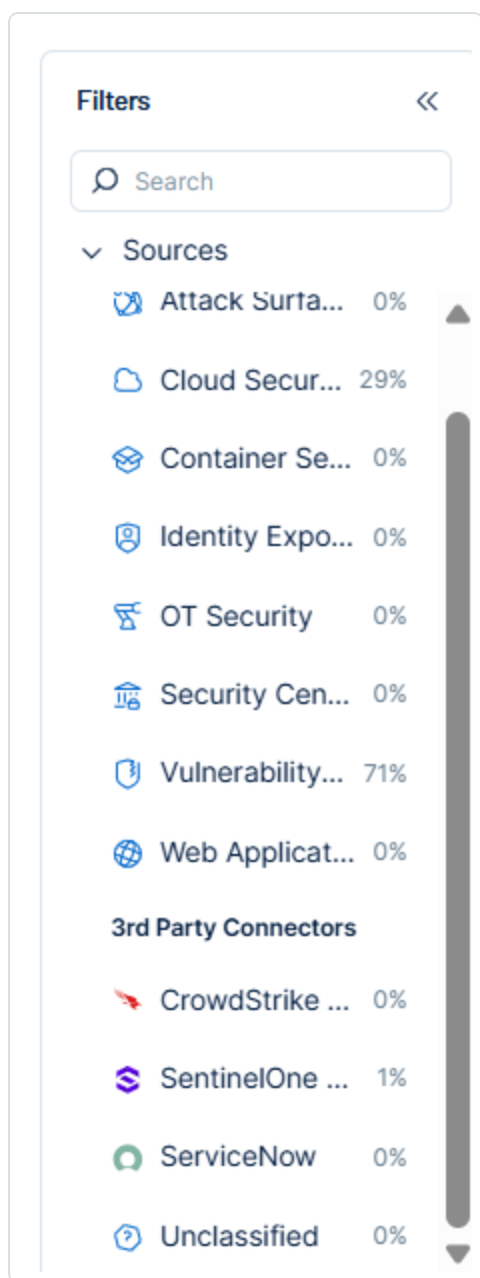
## Acunetix Premium in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

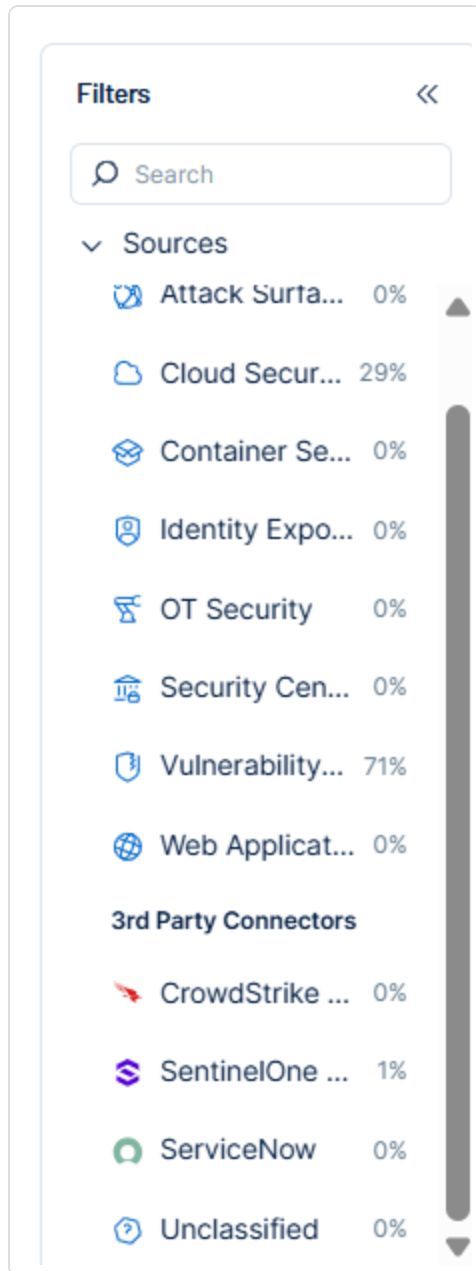
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

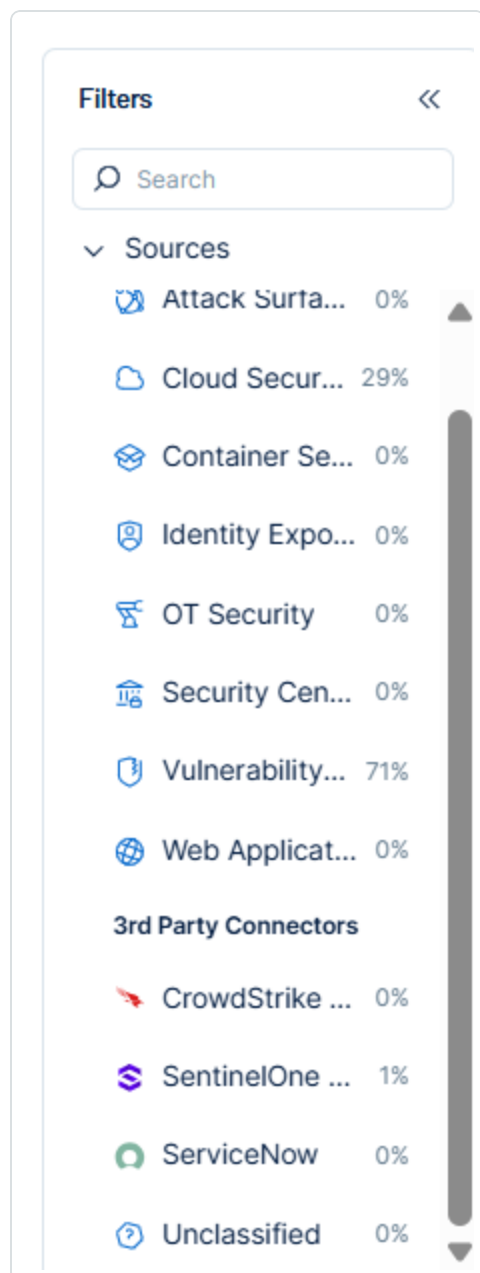
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

### Web Application Mapping

Tenable Exposure Management Value	Acunetix Premium Value
Unique Identifier	target_id
Asset - Name	address
Asset - Last Observed At	last_scan_date
Asset - Webapp Homepage Screenshot Url	address
Asset - External Tags	Business criticality

### Finding Mapping

Tenable Exposure Management UI Field	Acunetix Premium Field
Unique Identifier	affects_url + affects_detail
Finding Name	vt_name
CWEs	CWE (when available)
Severity Driver	cvss_score
Description	description
First Seen	first_seen
Last seen (Observed)	last_seen
Finding Custom Attributes	impact



	CVSS2
	CVSS3
	url
	parameter
	http_request
	http_response
	details
	AcunetixCriticality
	AcunetixSeverity
	confidence

## Finding Status Mapping

Tenable Exposure Management Status	Acunetix Premium Status
Active	Open false_positive ignored
Fixed	fixed

**Note:** For Acunetix Premium, Exposure Management uses the Status field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	[Connector] Score
Critical	<b>CVSS:</b> 9.0 - 10.0
High	<b>CVSS:</b> 7.0 - 8.9
Medium	<b>CVSS:</b> 4.0 - 6.9
Low	<b>CVSS:</b> 1-3.9



None

CVSS:0

**Note:** For Acunetix Premium, Exposure Management uses the `cvss_score` field to determine severity.

## API Endpoints in Use

API	Use in Tenable Exposure Management
{{ server_url }}/targets	Assets
{{ server_url }}/vulnerabilities	Findings
	Detections

## Armis Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The [Armis Asset Intelligence & Security Platform](#) aggregates, deduplicates, and normalizes asset data from your existing solutions to provide a consistently accurate inventory, uncover security gaps, and automate action – streamlining your operations.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Armis</a>
Category	OT (Operational Technology)
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices



Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

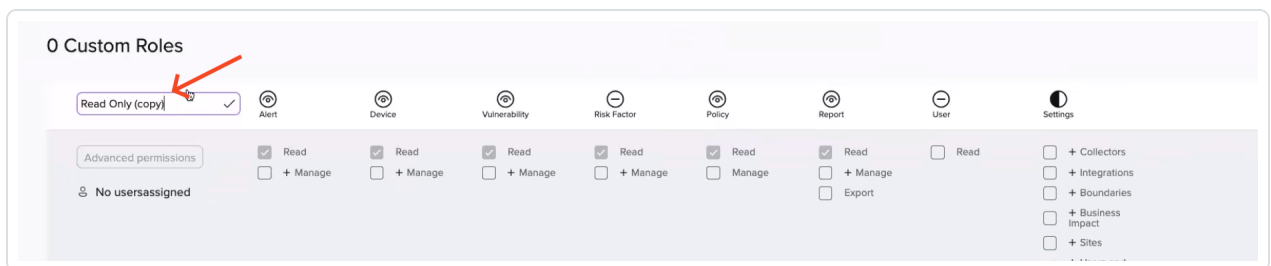
## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Identify your Armis account instance name.
- **Create a custom read-only role in Armis:**
  1. Sign in to the Armis portal.
  2. Navigate to **Settings > Roles & Permissions**.
  3. Under **Predefined Roles**, locate the **Read-only** role and click the copy icon to duplicate it.

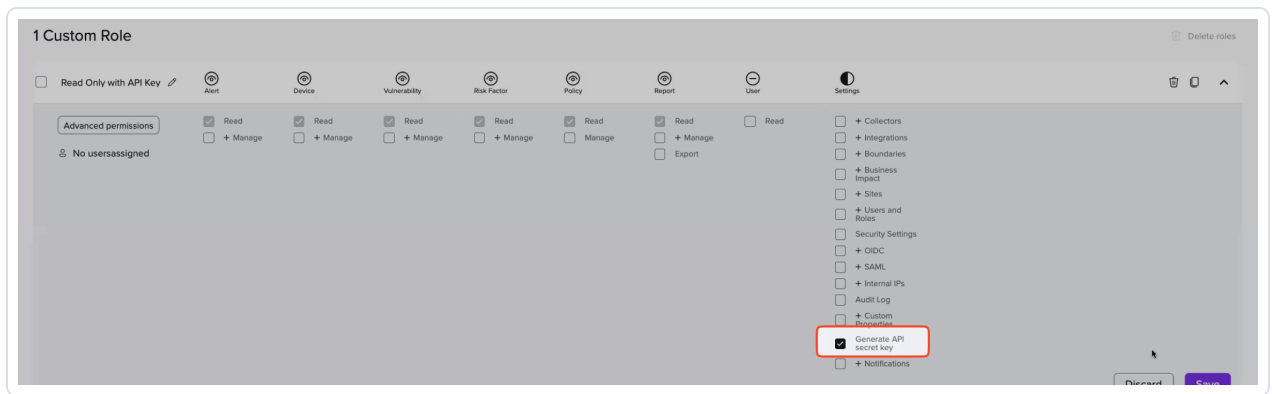


4. Update the name of the new role as needed.



5. Select the checkbox for **Generate API Secret Key** to enable API access.





### Create a new user in Armis:

1. Navigate to **Settings > Users**.
2. Click **Add User**.
3. Fill in the required fields:
  - Name – Enter a name of your choice.
  - Username – Enter a preferred username.
  - Email – Enter the user's email address.



- Roles – Select the read-only role created in the previous section.

**Roles**

Read Only with API Key

Filter

- ☐ Admin
- ☐ Read Only
- ☐ Security Analyst
- ☐ Asset Manager
- ☐ Integrations Manager
- ☐ User Manager
- ☒ Read Only with API Key

Only

4. Under **Allowed Sites**, choose either:

- **All Sites** – To ingest assets from all sites, or
- **Specific Sites** – To ingest only selected sites into Tenable Exposure Management.

5. Click **Add**.

A temporary password will be displayed. Make sure to save it securely.

- **Generate Armis API credentials:**

1. Navigate to **Settings > API Management**.
2. **Click Create to** create the secret key.
3. **Click Show** to access the secret key.
4. **Copy** the secret.


















Use the secret API Key and your Armis instance (i.e.,  
<https://yourarmisinstancename.armis.com>) to configure the connector.

## Add a Connector

To add a new connector:

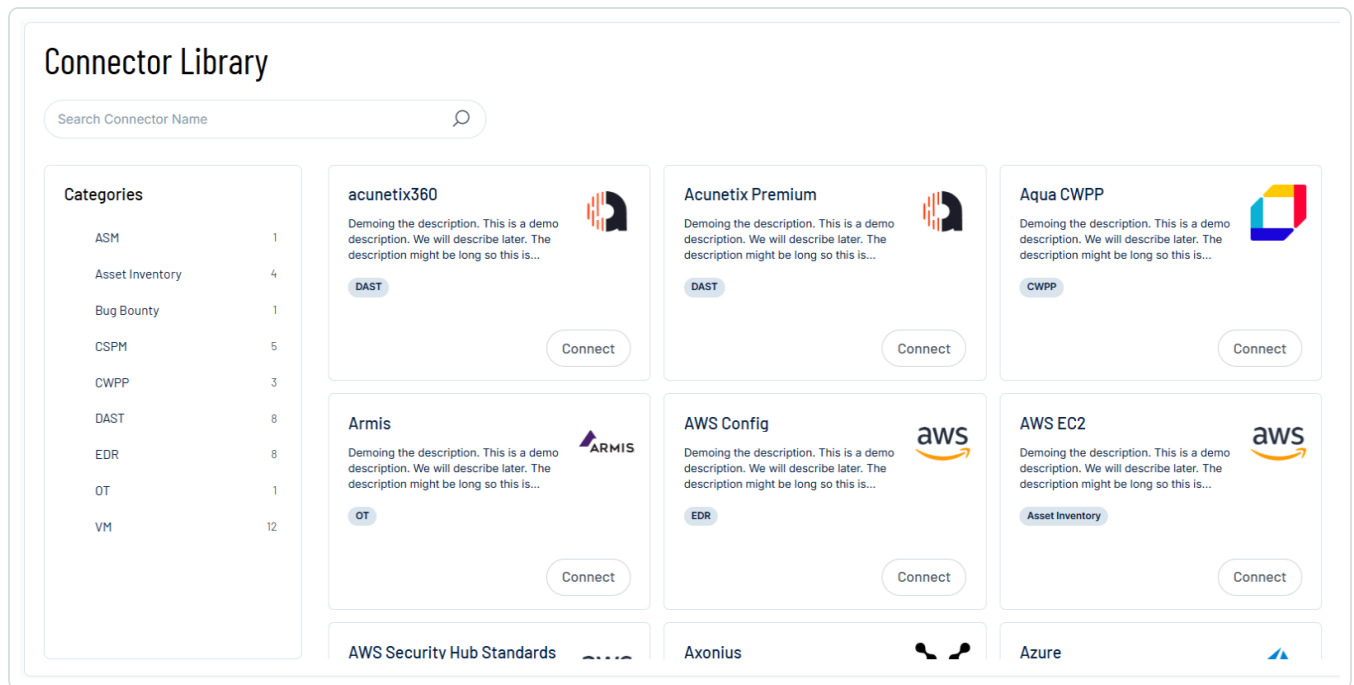
1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. Enter the credentials you generated earlier (API Key and your Armis instance name).
4. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.



- **Device categories to fetch:** Select the categories you want to fetch. The connector setup allows you to fetch all the existing asset categories in Armis except for the ones mentioned in [Support and Expected Behavior](#).
- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

❌ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✅ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:



- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.

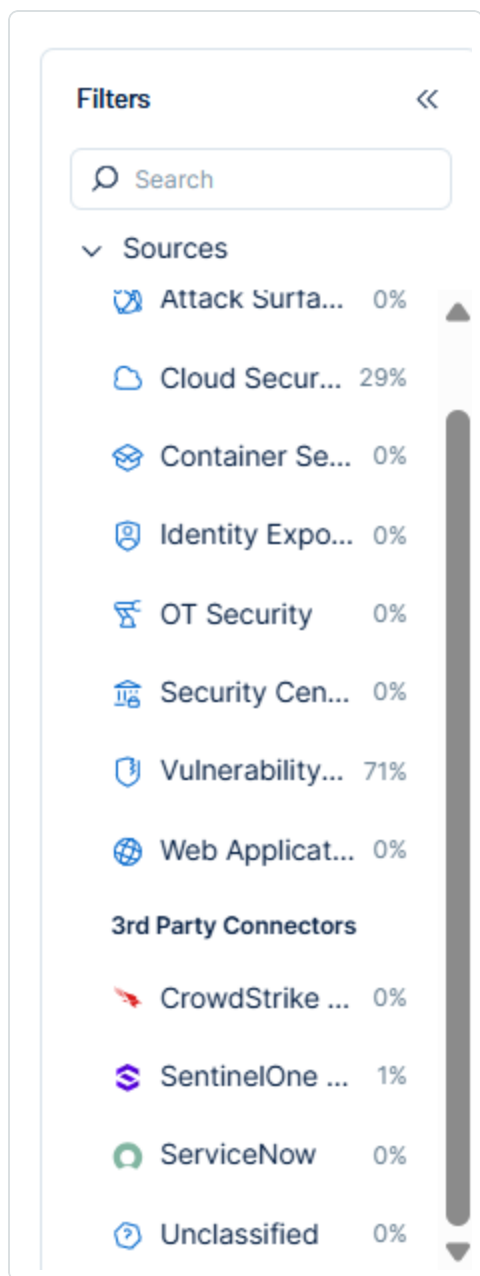
## Armis in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

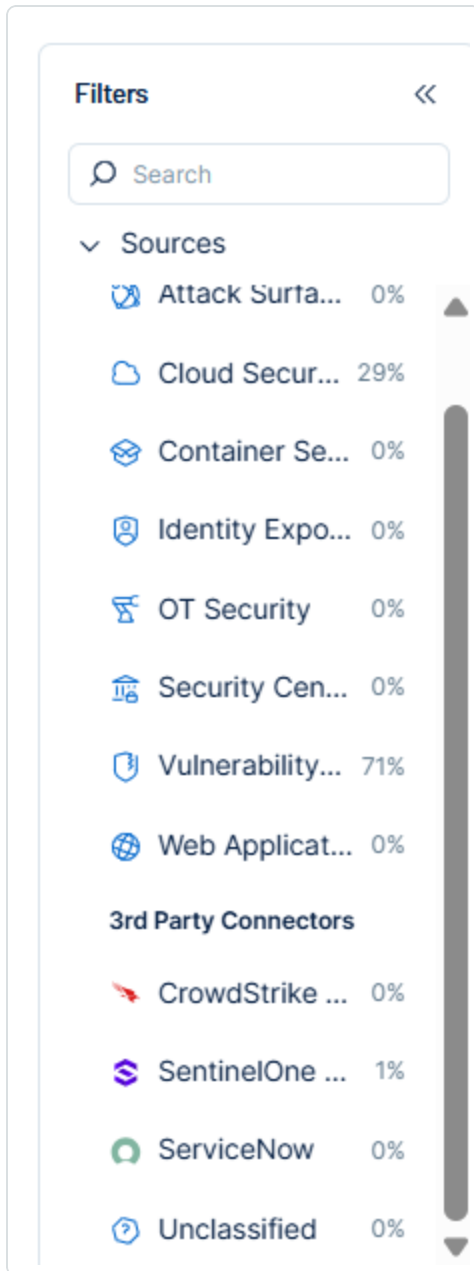
## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:



1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings



The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping





Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Armris Field
Unique Identifier	id
Asset - External Identifier or Asset - Provider Identifier	awsInstanceId or ibmCloudId or azureVmIdentifier
Asset - Name	name or names or macAddress or ipAddress or id
Asset - Operating Systems	operatingSystem
Asset - IPv4 Adresses Asset - IPv6 Adresses	ipAddress
Asset - MAC Addresses	macAddress
Asset - First Observation Date	firstSeen
Asset - Last Observed At	lastSeen
Asset - External Tags	tag  site.name  boundaries: boundary  category  type  sensor.name  sensor.type  businessImpact



	<code>riskLevel</code>
Asset Custom Attributes	<code>operatingSystemVersion</code> <code>armis_id: id</code> <code>site.name</code> <code>boundaries</code> <code>category</code> <code>type</code> <code>businessImpact</code> <code>riskLevel</code> <code>sensor.name</code> <code>sensor.type</code>

## Finding Mapping

Tenable Exposure Management UI Field	ArmIS Field
Unique Identifier	Alerts: <code>title + deviceId + alertId</code> Vulnerabilities: <code>cveUid + deviceId</code>
Finding Name	<code>cveUid</code> or <code>title</code>
CVEs	<code>cveUid</code>
Severity Driver	<code>cvssScore</code> or <code>severity</code>
Description	<code>data.description</code> or <code>description</code>
Finding Custom Attributes	<code>data.attackVector</code> <code>alert_id: alertId</code> <code>severity</code>



	<code>matchCriteriaString</code> <code>avm_rating: avmRating</code> <code>confidenceLevel</code> <code>vulnerability_type: vuln_type</code> <code>severity: severity_value or severity</code> <code>type</code> <code>number_of_threat_actors:</code> <code>numberOfThreatActors</code> <code>user_interaction: userInteraction</code> <code>privileges_required: privilegesRequired</code> <code>has_ransomware: hasRansomware</code> <code>is_weaponized: isWeaponized</code> <code>attack_complexity: attackComplexity</code> <code>availability_impact: availabilityImpact</code> <code>confidentiality_impact:</code> <code>confidentialityImpact</code> <code>integrity_impact: integrityImpact</code> <code>epss_score: epssScore</code> <code>exploitability_score: exploitabilityScore</code> <code>impact_score: impactScore</code>
First Seen	<code>firstDetected</code>
Last seen (Observed)	<code>lastDetected</code>

## Finding Severity Mapping

<b>Tenable Exposure Management Severity</b>	<b>Armis Score</b>
---	--------------------



Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:**For Armis, Tenable uses the `cvssScore` field to determine severity. If `cvssScore` is not available, Tenable uses the `severity` field from the connector, if provided.

## Finding Status Mapping

Tenable Exposure Management Status	Armis Status
Active	open or unhandled
Fixed	resolved

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
------------------------------------	-------------------



Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <b>resolved</b>, <b>ignored</b>, or <b>suppressed</b> on the vendor's side.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Detection	title or cveUid
Finding	title + deviceId + alertId or cveUid + deviceId

## Support and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

Exposure Management ingests Devices from Armis across all categories, except the following:



- Inputs
- Server Rack Components (ServerRackComponent)
- Other (Unknown)

These device categories will not appear in Exposure Management.

## API Endpoints in Use

API version: 1.0

API	Use in Tenable Exposure Management
https://{ armis_instance }.armis.com/api/v1/access_token/	Auth
https://{ armis_instance }.armis.com/api/v1/search/	Assets, Detections, Findings
https://{ armis_instance }.armis.com/api/v1/vulnerability-match/	Detections, Findings

## Data Validation

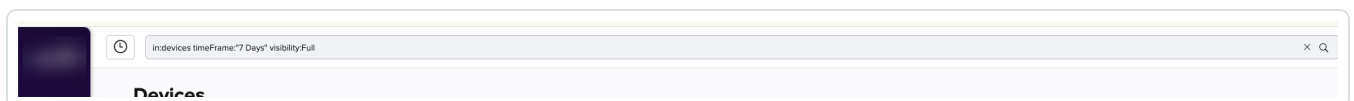
This section shows how to validate and compare data between Tenable Exposure Management and the Armis platform.

### Asset Data Validation

**Objective:** Ensure the number of devices in **Armis** aligns with the number of devices displayed in Tenable Exposure Management.

In Armis:

1. Navigate to **Assets > Devices**.
2. Click on the search bar at the upper portion of the screen.





3. Update the **Time Frame** to match the [archiving settings](#) (asset retention) in Tenable Exposure Management.
4. Remove the **Visibility** filter.
5. Click **+Add Filter** and choose **Category**.

bility:Full

Time Frame

= 7 x Days ▾

Visibility

= Full x ▾

+ Add Filter ▾

cat

Category

Properties

AD Location

Properties / Additional Properties

AD No Pre Authentication Required

Properties / Additional Properties

AP Location

Properties / Additional Properties

Access Point Location

Properties / Additional Properties

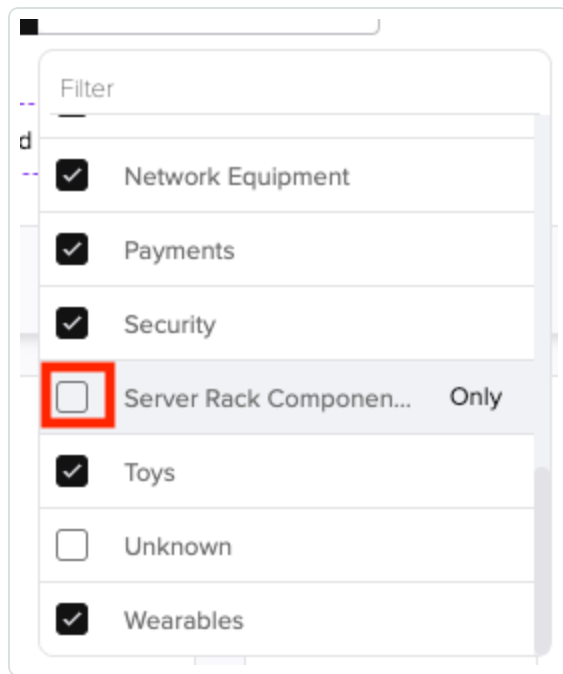
Device Location

Properties / Additional Properties

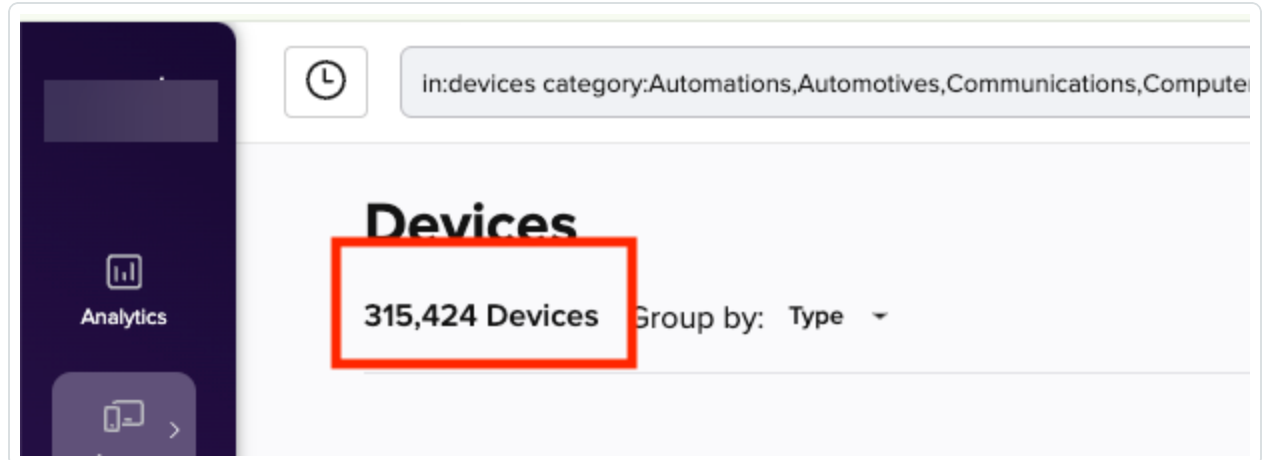
Last Connected AP Location

Properties / Additional Properties

6. Set the categories to align with those configured in Tenable Exposure Management, *excluding* **"Input"**, **"Server Rack Components"**, and **"Unknown"**.



7. Click outside the search bar to apply the filter.
8. Under the title **Devices**, you will see the number of assets that should appear for the connector in Tenable Exposure Management.



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Armis and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Armis and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:





- Archived based on the last observed date (field `lastSeen`)
- Archived because it did not return in the connector's next sync.

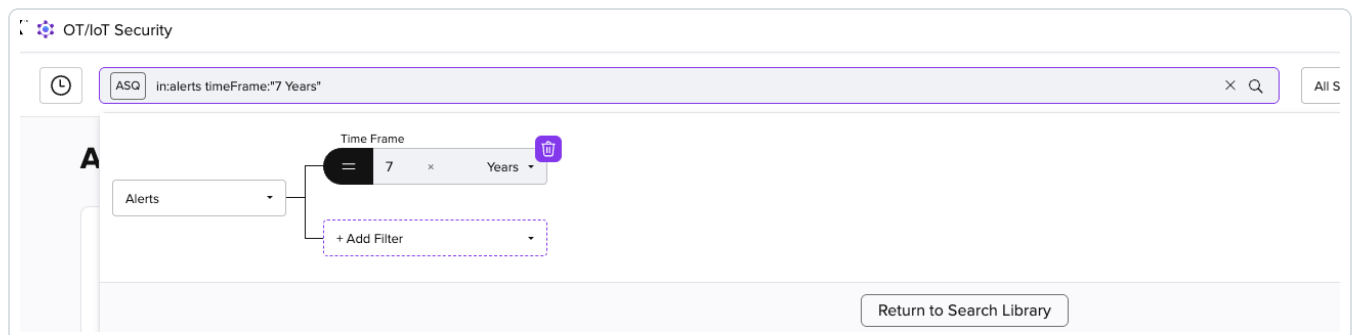
**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure the number of findings in Armis aligns with the number of findings in Tenable Exposure Management. Exposure Management retrieves both "**Alerts**" and "**Vulnerabilities**" from Armis.

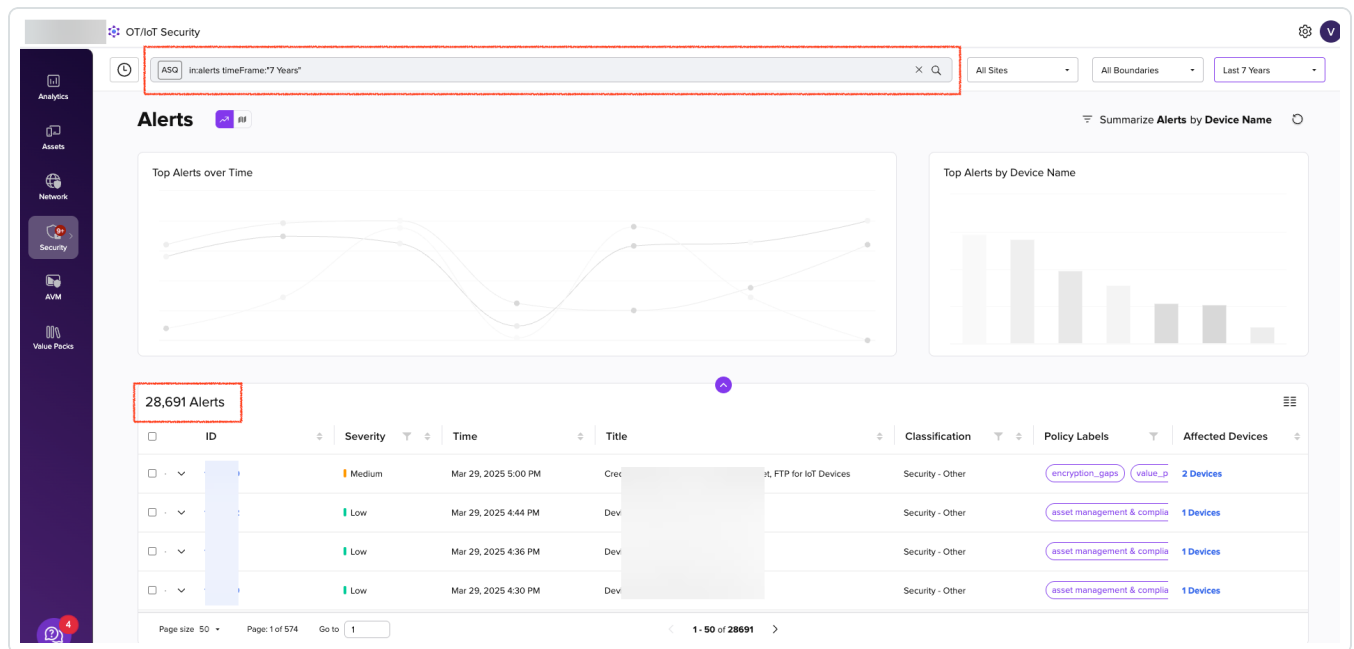
To access "Alerts" in Armis:

1. Navigate to **Security > Alerts**.
2. Filter the results using the **ASQ** at the top of the page. Set the **Time Frame** to at least the first time you started using the Armis platform to capture all relevant alerts.



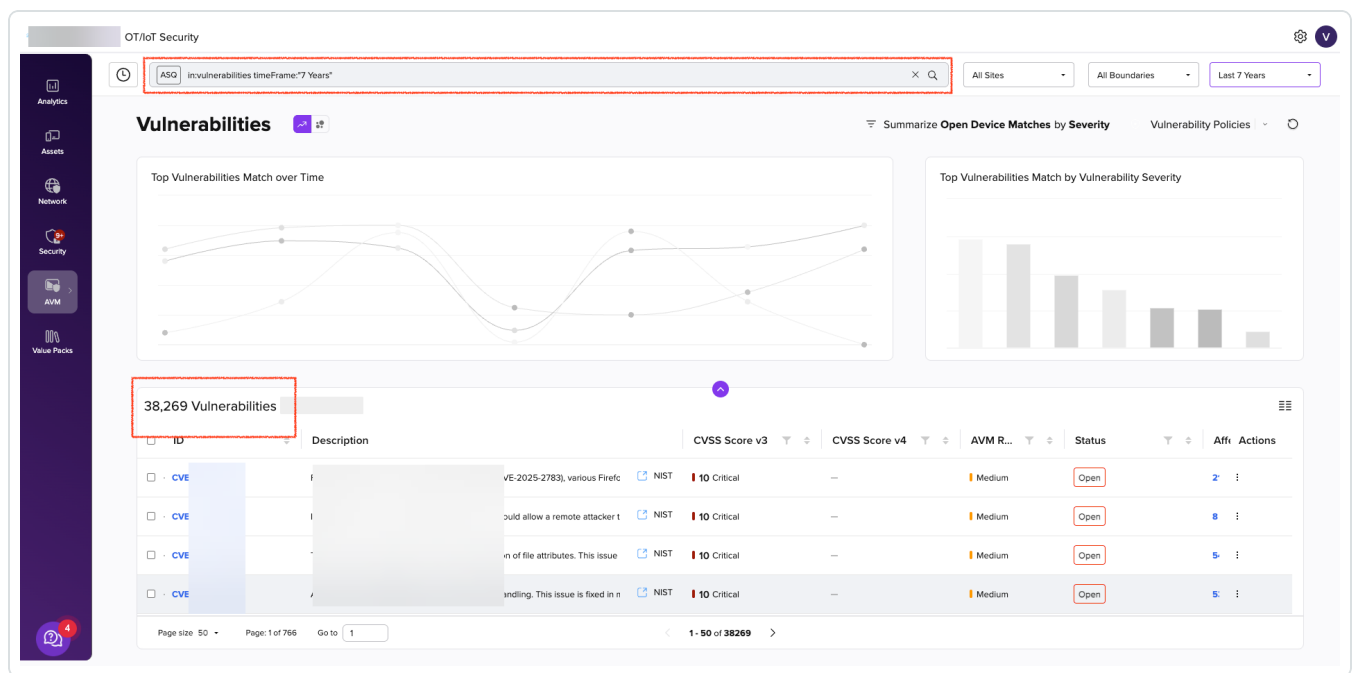


The number of Alerts will appear.



To access "Vulnerabilities" in Armis:

1. Navigate to **AVM > Vulnerabilities**.
2. Filter the results using the **ASQ** at the top of the page. Set the **Time Frame** to at least the first time you started using the Armis platform to capture all relevant vulnerabilities.



The total number should represent the vulnerabilities present in your system.

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between Armis and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Armis (Alerts + Vulnerabilities) and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

AWS EC2 Connector



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Amazon Elastic Compute Cloud \(Amazon EC2\)](#) is a core service provided by Amazon Web Services (AWS) that allows users to run virtual machines (called instances) in the cloud. These instances can be used to host applications, run batch jobs, serve websites, or perform virtually any compute-related task—without needing to own or manage physical hardware.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Amazon Elastic Compute Cloud (AWS EC2)</a>
Category	Asset Inventory
Ingested data	Assets only
Ingested <a href="#">Asset Classes</a>	Devices Resources
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

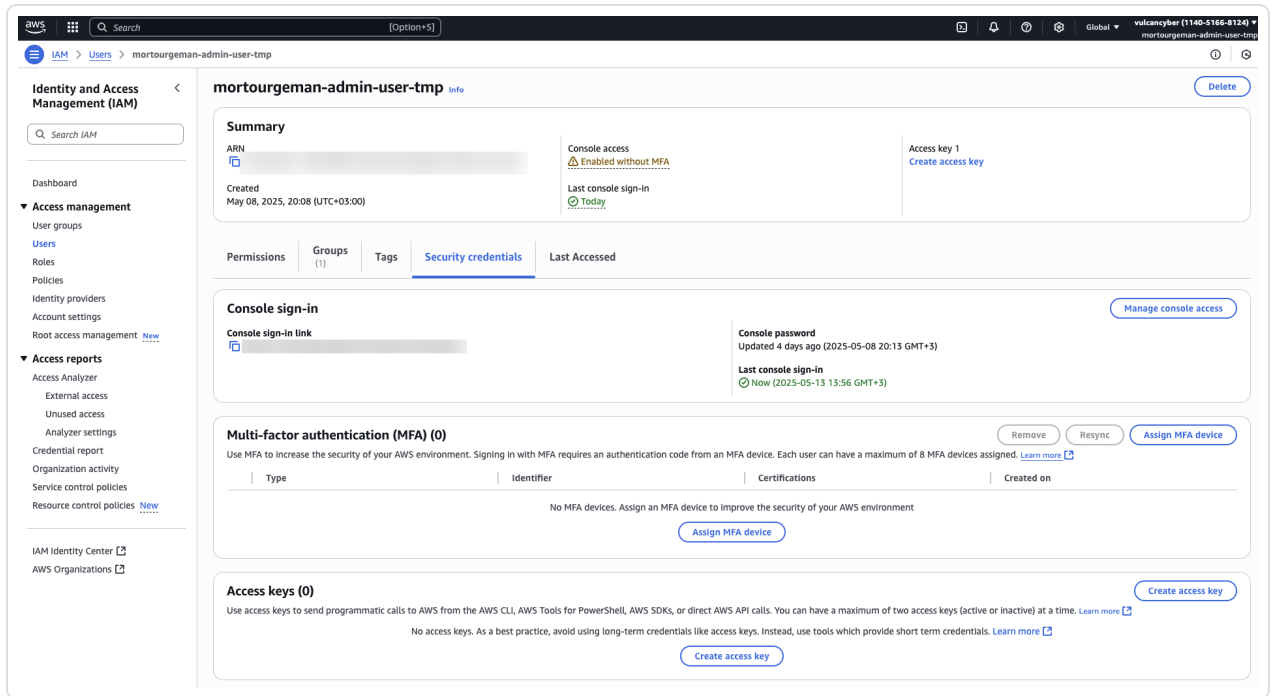
Before you begin configuring the connector, make sure to:

- **Create a cross-account role in AWS with the required access permissions:**
  - ec2:DescribeSecurityGroups
  - ec2:DescribeInstances



## Generate AWS secret and access keys and grant required permissions:

1. Login with the target account credentials to the AWS Console.
2. Navigate to **IAM > Users**.
3. Select the user with the appropriate permissions.



4. Navigate to the **Security Credentials** tab.
5. In the **Access Keys** section, click **Create access key**.  
A **Create access key** wizard appears.
6. In the **Use case** section, select the **Third-party service** radio button.
7. Click **Next**.
8. In the **Description tag value** text box, type a descriptive tag for the key.
9. Click **Create access key**.
10. Save the **Access key** and **Secret key** values for use within Tenable Exposure Management.



- **Obtain the ARN and external ID for the cross-account role:**

To include data from both your main AWS account and any linked accounts (enabling cross-account access), you must generate an ARN and External ID to configure the connector within Tenable Exposure Management.

**Important:** If you're creating roles for multiple AWS accounts, you must repeat these generation steps for each individual account.

You must also:

- Use the same External ID for all roles.
- When configuring the connection in Tenable, if you're entering multiple ARNs, separate them with commas, for example, `arn:aws:iam::123456789012:role/TenableRole,arn:aws:iam::098765432109:role/TenableRole`.

In the AWS Console:

1. Navigate to **IAM > Policies > Create Policy > Visual Editor**.
2. From the **Service** drop-down, select the appropriate EC2 service.

The screenshot shows the 'Specify permissions' page in the AWS IAM console. On the left, a progress bar indicates 'Step 1: Specify permissions' is active, followed by 'Step 2: Review and create'. The main area is titled 'Specify permissions' with a subtitle 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' Below this is the 'Policy editor' section with tabs for 'Visual', 'JSON', and 'Actions'. The 'Visual' tab is selected. Under 'Select a service', there's a search bar and a list of 'Commonly used services'. The 'EC2' service is highlighted in the list. At the bottom right, there are 'Cancel' and 'Next' buttons.

3. From the **Actions allowed** drop-down, select the following permissions:
  - **DescribeInstances**
  - **DescribeSecurityGroups**



4. Click **Next: Review**.
5. On the **Review policy** page, type a **Name** and **Description** for the policy.
6. Review the **Summary**.
7. Click **Create Policy**.
8. Navigate to **IAM > Roles > Create Role > Another AWS account**.
9. In the **Account ID** field, paste the following Tenable account ID:

012615275169

10. Select the **Require External ID** check box.

The screenshot shows the AWS IAM console 'Create role' page. The breadcrumb navigation is 'IAM > Roles > Create role'. The left sidebar shows the progress: 'Add permissions', 'Step 3', and 'Name, review, and create'. The main content area is titled 'Trusted entity type' and contains five options: 'AWS service', 'AWS account' (selected), 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below this, the 'An AWS account' section is expanded, showing 'This account (114051668124)' and 'Another AWS account' (selected). The 'Account ID' field is populated with '012615275169'. Under the 'Options' section, the 'Require external ID (Best practice when a third party will assume this role)' checkbox is checked. A note explains that this option increases security by preventing 'confused deputy' attacks.

11. In the text box, type the value of your external ID.
12. Paste this value into the **Connector** text box.
13. Ensure the **Require MFA** check box is deselected.
14. Click **Next: Permissions**.
15. Attach the policy you created.
16. Continue through the wizard and review the settings.



17. Create the role.

18. Copy the generated **ARN** for use within Tenable Exposure Management.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

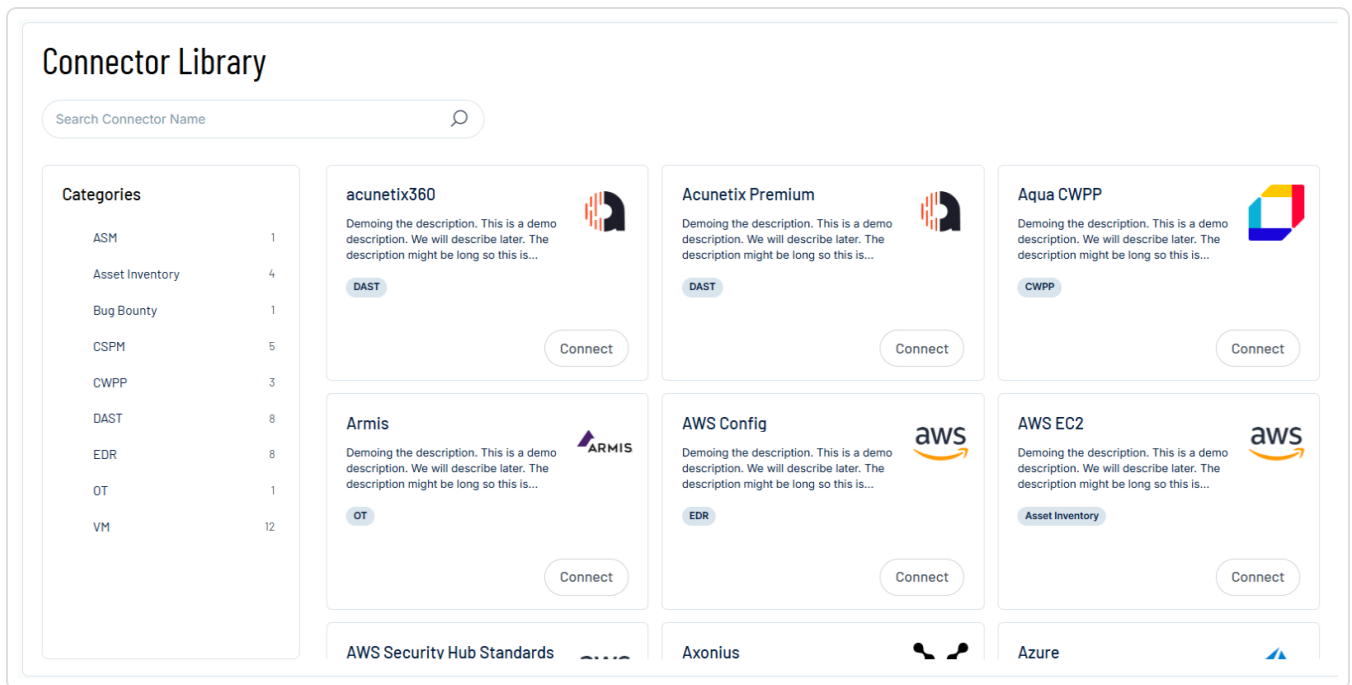
Add new connector

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.





3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Regions** text box, type a comma separated list of the cloud regions in which your AWS accounts reside.
4. Do one of the following:



- For a single AWS account:
  - a. In the **Access Key** Integration section, in the **Access Key** and **Secret Key** text boxes, paste the access and secret keys [generated in AWS](#).
- For multiple AWS accounts:
  - a. In the **ARN integration** section, in the **External ID** text box, type the external ID for your AWS account.
  - b. In the **ARNs** text box, type a list of comma separated ARNs from which you want to pull AWS data.

**Important!** At least one of the provided ARNs must have access to each selected region to allow successful data collection.

**Note!** Exposure Management attempts to sync each selected region using all available ARNs. Partial coverage is supported, but at least one ARN must have access to every selected region to ensure complete data ingestion.

5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

✔ Successful tests 3 out of 4 integration tests succeeded

[Test connectivity](#)  
[Show tests](#) ▼  
[Show tests](#) ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

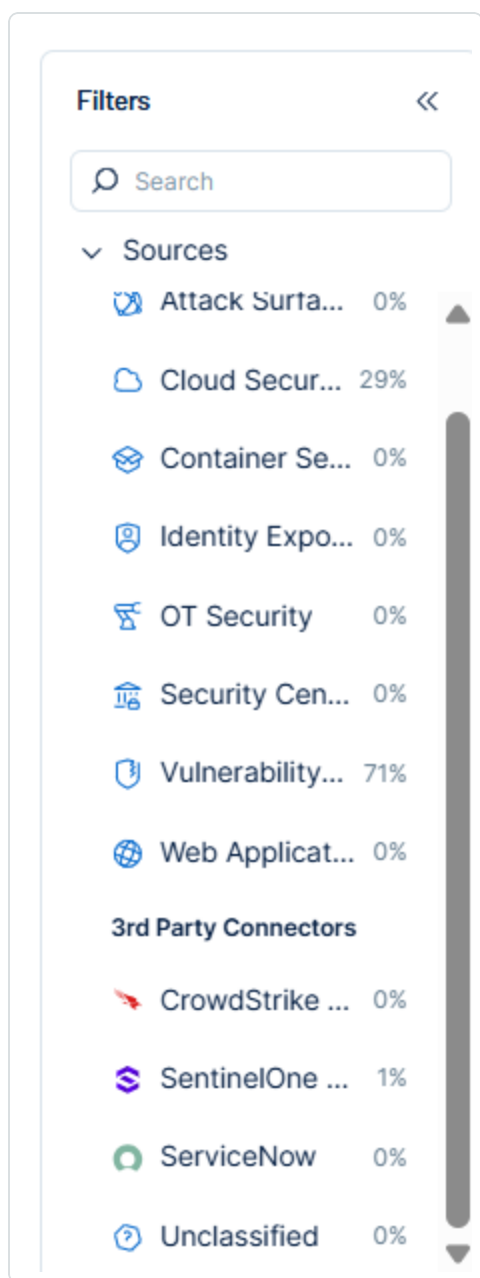
## AWS in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



Tenable Exposure Management UI Field	AWS EC2 Field
Unique Identifier	InstanceId
Asset - External Identifier or Asset - Provider Identifier	InstanceId
Asset - Name	PublicDnsName or InstanceId
Asset - Operating Systems	Platform or PlatformDetails
Asset - IPv4 Adresses	PrivateIpAddress
Asset - IPv6 Adresses	PublicIpAddress
Asset - MAC Addresses	MacAddress
Asset - Host Fully Qualified DNS	PrivateDnsName
Asset - First Observation Date	LaunchTime
Asset - External Tags	Tags
Asset Custom Attributes	AvailabilityZone InstanceType SecurityGroups AmiLaunchIndex KeyName

## Resource Mapping

Tenable Exposure Management UI Field	AWS EC2 Field
Unique Identifier	GroupId
Asset - Name	GroupName
Provider Names	AWS



Cloud Resource Type	AWS::EC2::SecurityGroup
Asset - External Identifier or Asset - Provider Identifier	GroupId
Asset - External Tags	Tags
Asset Custom Attributes	VpcId OwnerId

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li><li>(Configurable) Asset status (<code>State.Name</code>) changes to one of the selected statuses defined in the Asset Retention configuration: <code>pending</code>, <code>running</code>, <code>shutting-down</code>, <code>terminated</code>, <code>stopping</code>, <code>stopped</code>. The status <code>terminated</code> is selected by default.</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>[Finding no longer appears in the scan findings]</li><li>[Finding status changes to <code>[resolved]</code>, <code>[ignored]</code>, or <code>[suppressed]</code> on the vendor side]</li><li>[Findings status on the connector's side indicates irrelevancy (e.g., "<code>[INACTIVE]</code>")]</li></ul>



**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Supported Asset Types

The AWS EC2 connector fetches data only for the following asset types:

- EC2 Instances
- Security Groups

### API Endpoints in Use

API version: 11.3.0

API	Use in Tenable Exposure Management	Required Permissions
describe_instances	generating Devices	EC2 describeInstances
describe_security_groups	generating Resources	EC2 describeSecurityGroups

### Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the AWS EC2 platform.

#### Asset Data Validation

**Objective:** Ensure the number of assets in AWS EC2 aligns with the number of devices displayed in Tenable Exposure Management.

In AWS EC2 :



1. Navigate to **EC2 > Instances**.
2. Ensure that **all instance states** are selected.
3. Review the total number of EC2 instances.

Note the number of terminated instances. These are archived by default and do not appear Exposure Management.

4. Subtract the terminated instances from the total to get the count of active instances expected in Exposure Management.

In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between AWS EC2 and Tenable Exposure Management.

**Expected outcome:** The asset count in Exposure Management may not perfectly match those in AWS EC2, as the connector captures data via periodic snapshots rather than real-time updates. Discrepancies can occur due to instance changes between syncs, short-lived instances, regional filtering, or IAM permission limitations.

## Security Groups (Resources) Data Validation

**Objective:** Ensure the number of assets in AWS EC2 aligns with the number of resources displayed in Tenable Exposure Management.

In AWS EC2:

1. Navigate to **EC2 > Network & Security > Security Groups**.
2. Review the total number of security groups.

In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of resources between AWS EC2 and Tenable Exposure Management.

**Expected outcome:** Resources listed AWS EC2 should match those shown in Exposure Management.





If an asset is not visible in Exposure Management, check the following conditions:

- The asset status changed to one of the selected statuses defined in the Asset Retention configuration.
- The asset was archived based on the last observed date (last seen).
- The asset was archived based its status.
- The asset was archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## AWS Inspector V2 Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The AWS Inspector Connector enumerates vulnerabilities from AWS Inspector, ECR, and ECS.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">AWS Inspector</a>
Category	Asset Inventory Network Scanner
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Device Container Resource



Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

1. Have a cross-account user with the permission: **inspector2:ListFindings**
2. Complete **one** of the following configurations based on your use case:

- **Generate AWS Inspector V2 Access and Secret Keys (for Access and Secret Key authentication method):**
  1. Sign in to the AWS Management Console as an IAM user with administrative privileges (not the root account).
  2. Navigate to the **IAM** Console: <https://console.aws.amazon.com/iam>
  3. In the left navigation pane, select **Users**.
  4. Select the cross-account user with the **inspector2:ListFindings** permission.
  5. Choose the **Security credentials** tab.
  6. In the Access keys section, click **Create access key**.
  7. In the **Access key best practices and alternatives**, select **Third-party service** as the use case.

aws Search [Option+S]

IAM > Users > mortourgeman-admin-user-tmp > Create access key

Step 1  
☒ Access key best practices & alternatives  
 Step 2 - optional  
☐ Set description tag  
 Step 3  
☐ Retrieve access keys

### Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

**Use case**

- ☐ **Command Line Interface (CLI)**  
You plan to use this access key to enable the AWS CLI to access your AWS account.
- ☐ **Local code**  
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- ☐ **Application running on an AWS compute service**  
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- ☒ **Third-party service**  
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- ☐ **Application running outside AWS**  
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
- ☐ **Other**  
Your use case is not listed here.

**Alternative recommended**  
 As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys. [Learn more](#)

**Confirmation**  
☒ I understand the above recommendation and want to proceed to create an access key.

[Cancel](#) [Next](#)

8. Click **Next**.

9. In the **Set description tag**, add a description tag (e.g., Exposure Management Intergation).

10. Click **Create access key**.

11. On the confirmation page, copy the:

- **Access Key ID**
- **Secret Access Key**

You won't be able to view the Secret Access Key again after this screen, so save it securely.

• **Create AWS Inspector V2 External ID and ARNs (for ARN and External ID authentication method):**



1. Sign in to the AWS Management Console with an account that has permissions to create IAM policies.
2. Navigate to the **IAM** service.
3. In the left-hand menu, click on **Policies**, then click **Create policy**.
4. In the **Create Policy** page, select the **Visual editor** tab.
5. Under **Service**, search for and select **Inspector2**.
6. Under **Actions**, select the **inspector2:ListFindings** permission.
7. Click **Next: Review**.
8. On the **Review policy** page, enter a **Name** and (optionally) a **Description** for the policy.
9. Review the Summary to ensure the correct permissions are included.
10. Click **Create policy** to save.
11. Navigate to **IAM > Roles > Create Role > Another AWS account**.
12. In the **Account ID** field, paste the following Tenable account ID: **012615275169**
13. Check the **"Require External ID"** box.
14. Enter your **External ID** value (maximum 12 characters).
15. Copy the value and save in a safe place so you can use it later in the connector setup page.

IAM > Roles > Create role

Step 1: Add permissions  
Step 2: **Add permissions**  
Step 3: Name, review, and create

### Trusted entity type

- ☐ AWS service: Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ **AWS account**: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.

### An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- ☐ This account (114051668124)
- ☒ **Another AWS account**

**Account ID**  
Identifier of the account that can use this role

012615275169

Account ID is a 12-digit number.

### Options

- ☒ **Require external ID (Best practice when a third party will assume this role)**  
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

16. Make sure "**Require MFA**" is *unchecked*.

17. Click **Next: Permissions**.

18. Attach the policy created in steps 2–8.

IAM > Roles > Create role

Step 1: Select trusted entity  
Step 2: **Add permissions**  
Step 3: Name, review, and create

### Add permissions

Permissions policies (1302)

Choose one or more policies to attach to your new role.

Filter by Type: All types | 39 matches

Search: ec2

<input type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	allowEc2AccessS3-vulcan-rhel-metadata	Customer managed	Allow Ec2 instances access the bucket ...

19. Continue through the wizard, review the role settings, and create the role.

20. Copy the generated ARN.

**Important:** If you're creating roles for multiple AWS accounts, repeat the steps above for each account. Make sure you use the same External ID for all roles and copy the generated ARN of each role/account.

Add a Connector

To add a new connector:



1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> ⋮
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> ⋮

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.

### Connector Library

#### Categories

ASM	1
Asset Inventory	4
Bug Bounty	1
CSPM	5
CWPP	3
DAST	8
EDR	8
OT	1
VM	12

acunetix360

Demoin the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoin the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoin the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoin the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoin the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoin the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.



The connector configuration options appear.

## Configure the Connector

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. From the Authentication method drop-down, select the authentication method to use for the connector.
  - If you select the **Access Key & Secret Key** method, enter the credentials you generated earlier.
  - If you select the **ARN & External ID** method, enter the credentials you generated earlier.
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - (Optional) In the Regions drop-down, select the AWS regions to include for data ingestion.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.



- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

⊗ Failed tests 1 out of 4 integration tests failed

Show tests ▾

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▾

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## AWS in Tenable Exposure Management

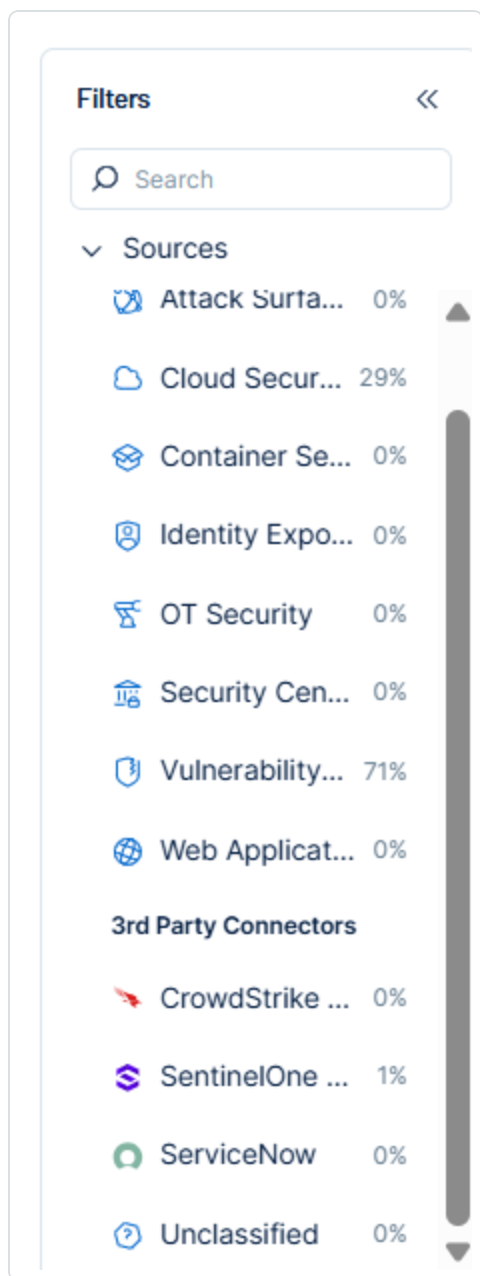
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.





The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

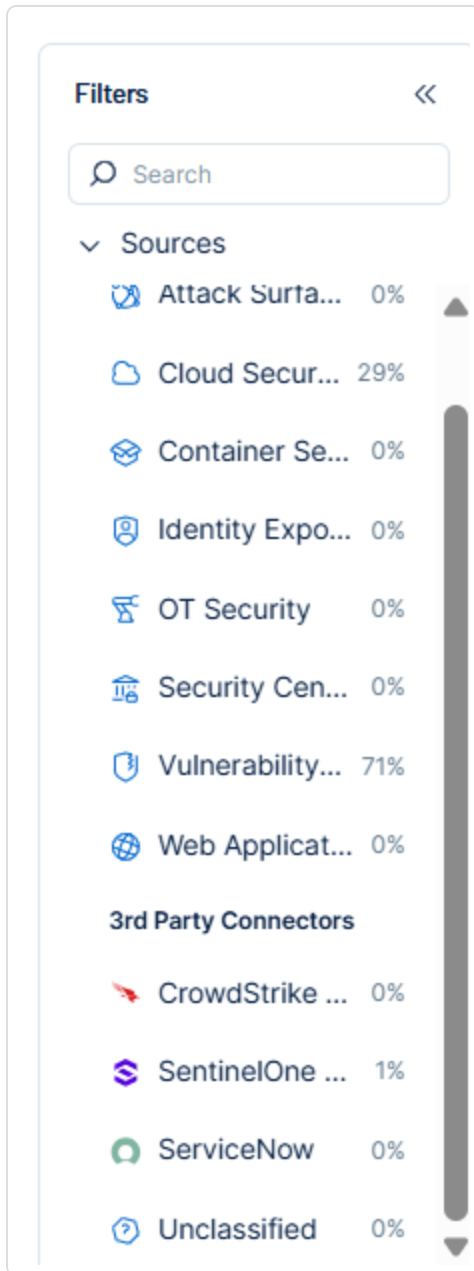
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

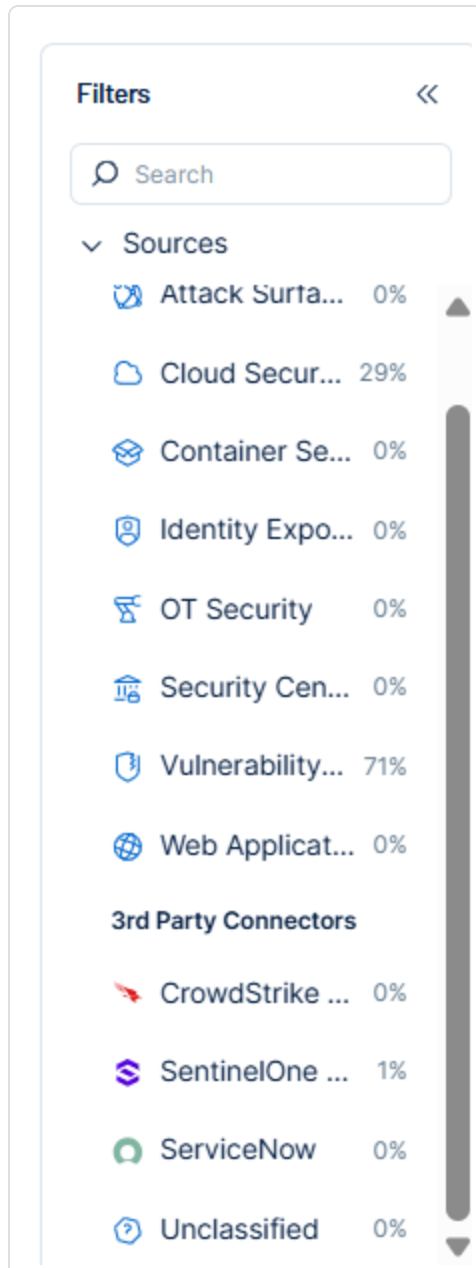
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	AWS Inspector V2 Field
Unique Identifier	id
Asset - External Identifier	id
Asset - Provider Identifier	
Asset - Name	tags.Name
Asset - Operating Systems	Platform
Asset - IPv4 Adresses	ipV4Addresses
Asset - IPv6 Adresses	ipV6Addresses
Asset - First Observation Date	launchedAt
Asset - External Tags	Tags
Asset Custom Attributes	region type keyName

## Container Mapping

Tenable Exposure Management UI Field	AWS Inspector V2 Field
Unique Identifier	id



Asset - Name	tags.Name
Asset - Operating Systems	Platform
Asset - Container Image Tags	imageTags
Asset - Image Digest	imageHash
Asset - External Tags	Tags
Asset Custom Attributes	region
	repositoryName

## Resource Mapping

Tenable Exposure Management UI Field	AWS Inspector V2 Field
Unique Identifier	id
Asset - External Identifier	id
Asset - Provider Identifier	
Asset - Name	functionName
Provider Names	AWS
Cloud Resource Type	AWS::Lambda::Function
Asset - External Tags	Tags
Asset Custom Attributes	region

## Finding Mapping

Tenable Exposure Management UI Field	AWS Inspector V2 Field
Unique Identifier	finding_arn
Finding Name	title
CVEs	vulnerabilityId



Severity Driver	<code>inspectorScore</code>
Description	<code>description</code>
First Seen	<code>firstObservedAt</code>
Last seen (Observed)	<code>lastObservedAt</code>
Port	<code>openPortRange.begin</code>
Protocol	<code>protocol</code>
Finding Custom Attributes	<code>networkPath</code> (only for Device and Resource) <code>severity</code> <code>type</code> <code>vulnerablePackages.name</code> <code>vulnerablePackages.version</code> <code>source</code> <code>sourceUrl</code> <code>remediation</code> <code>scoringVector</code>

### Finding Status Mapping

Tenable Exposure Management Status	AWS Inspector Status
Active	All other statuses
Fixed	CLOSED SUPPRESSED

**Note:**For AWS Inspector, Exposure Management uses the status field to determine finding status.

### Finding Severity Mapping



Tenable Exposure Management Severity	AWS Inspector Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:** For AWS Inspector, Exposure Management uses the `inspectorScore` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li></ul>



- Finding status changes to **Status = SUPPRESSED** or **CLOSED** on the vendor side

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Finding	finding_arn
Detection	title

## API Endpoints in Use

API version: 11.3.0 aioboto3

API	Use in Tenable Exposure Management	Requested Permissions
list_findings	generating Devices generating Resources generating Containers generating Findings	Inspector2 ListFindings

## Data Validation





This section shows how to validate and compare data between Tenable Exposure Management and the AWS Inspector platform.

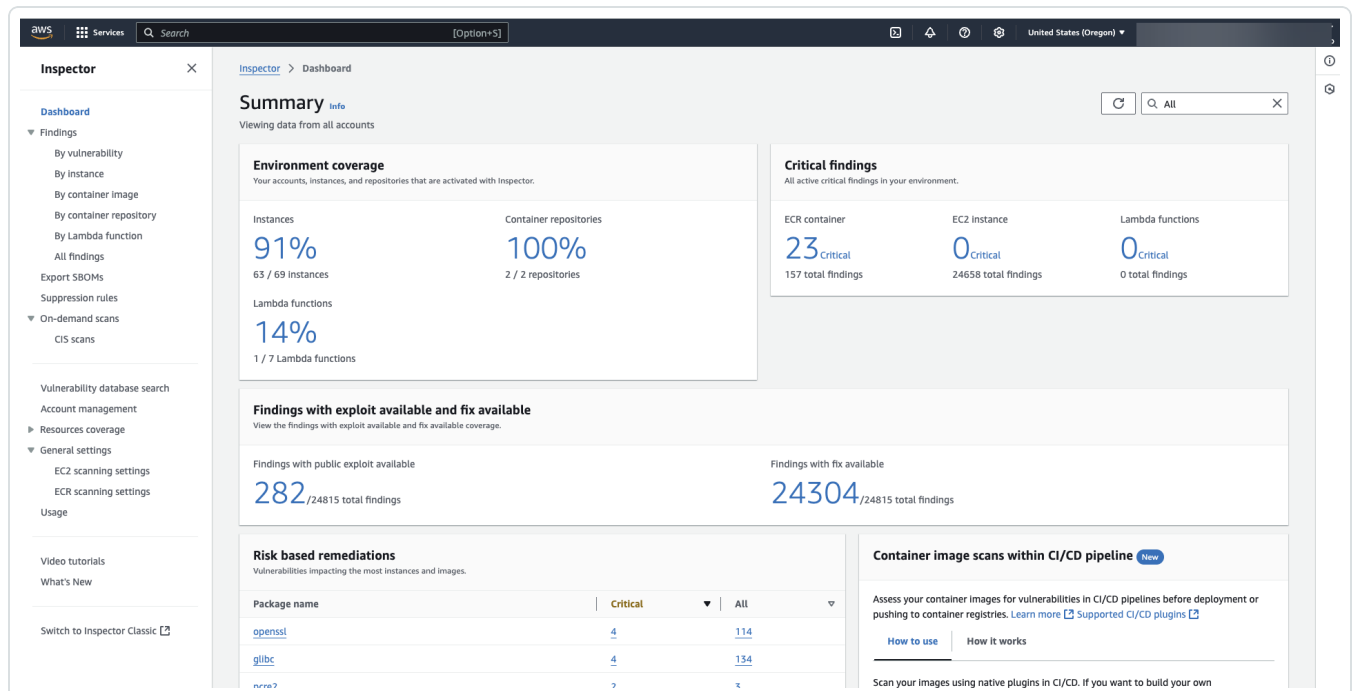
## Asset Data Validation

**Objective:** Ensure that the number of assets in AWS Inspector aligns with the number of assets displayed in Exposure Management.

In AWS Inspector:

1. Navigate to the **AWS Console > Amazon Inspector**.
2. In the left menu, click **Dashboard**.
3. Review the number of resources currently scanned and covered:
  - **EC2 instances**
  - **ECR container images**
  - **Lambda functions**

Each resource type is displayed in its own tile on the dashboard.



In Tenable Exposure Management:



1. [Locate your connector assets.](#)
2. Compare the total number of assets between AWS Inspector and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in AWS Inspector and Exposure Management should match.

Exposure Management displays assets from AWS Inspector if they are actively scanned.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on the last observed date (last seen).
- The asset was archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the number of findings in AWS Inspector aligns with the number of findings in Exposure Management.

In AWS Inspector:

1. Navigate to the **AWS Console > Amazon Inspector**.
2. On the **Dashboard**, review the **Findings** tile.
3. Focus on findings that:
  - Have an available exploit.
  - Have a recommended fix.

These represent the active vulnerabilities identified by AWS Inspector.

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between AWS Inspector and Tenable Exposure Management.



**Expected outcome:** Exposure Management ingests only findings with a defined exploitability and remediation. Counts may differ if some findings are informational or do not meet the ingest criteria.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## Axonius Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Axonius](#) is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies.

### Connector Details

Details	Description
Supported products	<a href="#">Axonius</a>
Category	Asset Inventory
Ingested data	Assets
Ingested <a href="#">Asset Classes</a>	Device
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version	SaaS (latest)



and type

## Prerequisites and User Permissions

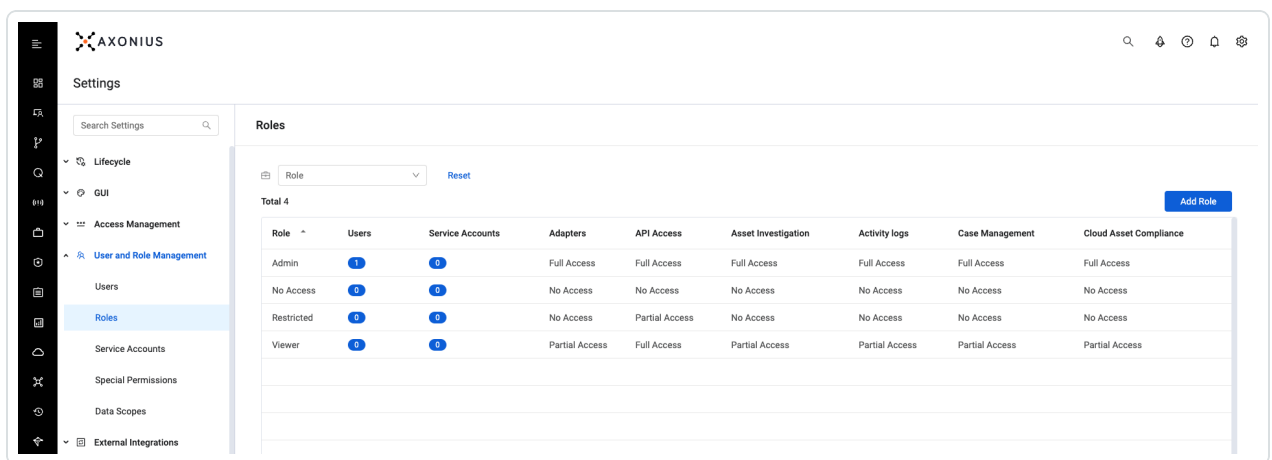
Before you begin configuring the connector, make sure to:

- Locate the Axonius Base URL for use in API requests (e.g., `https://<your-instance>.axonious.com`).

- **Create an Axonius user or service account with API access:**

For User Accounts:

1. In the upper right corner, click the gear icon to open System Settings.
2. Navigate to **User and Role Management > Roles**.



3. Select the relevant role.
4. Under API Access, ensure that Enable API Access is selected.
5. Click **Save**.

For Service Accounts:

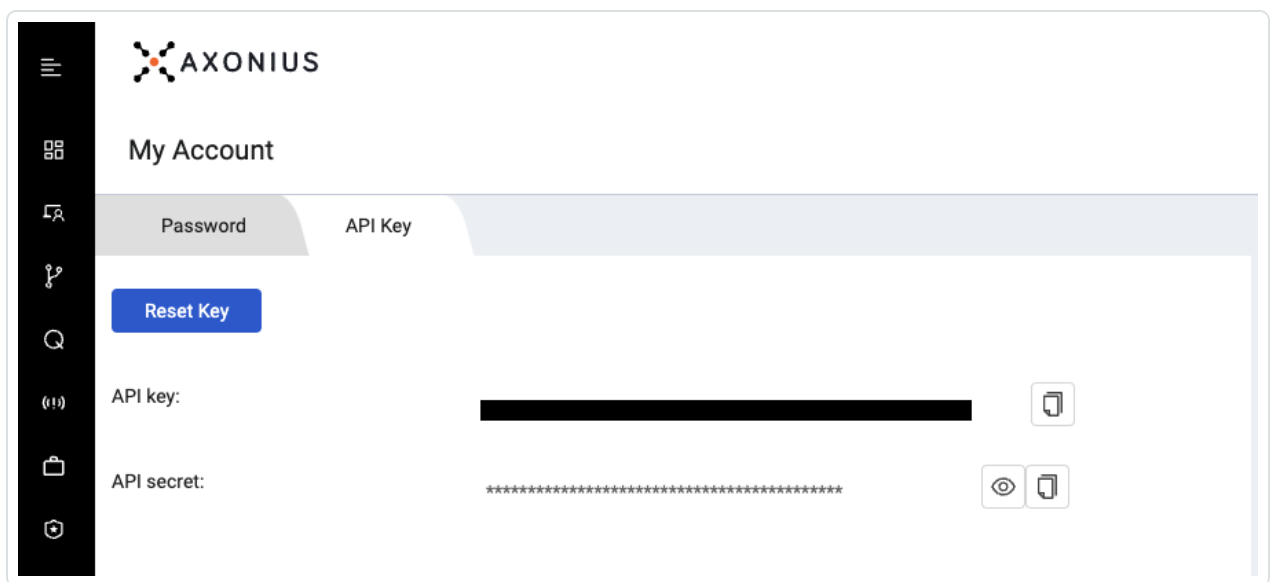
1. In System Settings, navigate to **User and Role Management > Service Accounts**.
2. Select the appropriate service account.
3. Confirm that it is assigned a role with API access permissions.



**TIP:** Permissions are assigned per role and the role is assigned to the service account. For more information see [Managing Service Accounts](#).

### Generate an Axonius API Key and Secret:

1. Click your user avatar at the bottom of the navigation panel and select **User Settings**.
2. Navigate to the **API Key** tab.
3. Copy your **API Key** and **API Secret**. You'll use these credentials to configure the connector in Exposure Management.



## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

DAST

Connect

Acunetix Premium

DAST

Connect

Aqua CWPP

CWPP

Connect

Armis

OT

Connect

AWS Config

EDR

Connect

AWS EC2

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

- 442 -



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server Url** section, type the URL of your Axonius server.
4. In the **API Access Key** and **API Secret Key** text boxes, paste the secret credentials you [generated in Axonius](#).
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Axonius in Tenable Exposure Management

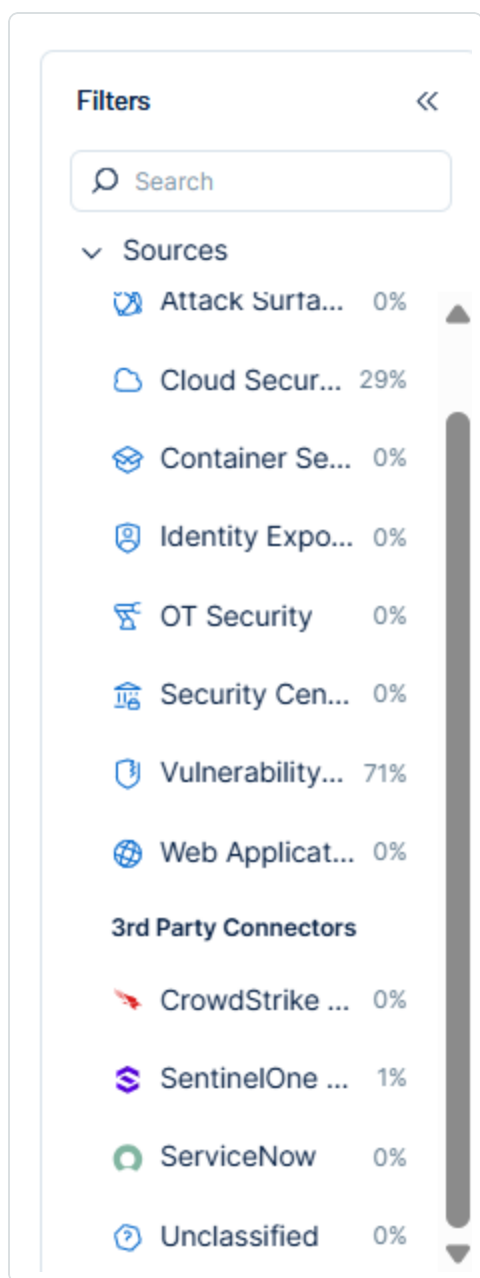
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.





The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



<b>Tenable Exposure Management UI Field</b>	<b>Axonious Field</b>
Unique Identifier	<code>internal_axon_id</code>
Asset - External Identifier or Asset - Provider Identifier	<code>specific_data.data.cloud_id</code>
Asset - Name	<code>specific_data.data.hostname_preferred</code> or <code>specific_data.data.name_preferred</code> or <code>specific_data.data.hostname_fqdn_preferred</code> or <code>specific_data.data.azure_display_name</code> or <code>specific_data.data.hostname</code> or <code>specific_data.data.name</code> or <code>specific_data.data.network_interfaces.ips_preferred[0]</code> or <code>internal_axon_id</code>
Asset - Operating Systems	<code>specific_data.data.os.type_preferred</code>
Asset - IPv4 Adresses Asset - IPv6 Adresses	<code>specific_data.data.network_interfaces.ips_preferred</code>
Asset - MAC Adresses	<code>specific_data.data.network_interfaces.mac</code>
Asset - Last Observed At	<code>specific_data.data.last_seen</code>
Asset - External Tags	<code>labels</code> and <code>adapters</code>



Asset Custom Attributes	<code>specific_data.data.os.os_str_preferre</code>
-------------------------	--

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	<code>internal_axon_id</code>

## API Endpoints in Use

API version: v1



See [Axonius Connector](#).

API	Use in Tenable Exposure Management	Requested Permissions
/api/devices/count	Getting total devices count for pagination proposes	Device Count
/api/devices	Fetching device assets	Devices

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Avoiding Sync Loops (Tenable Adapter in Axonius)

Axonius may include assets sourced from Tenable via its own Tenable adapter. To prevent sync loops—where assets originating from Tenable are re-ingested back into Tenable — the connector filters out any device whose only associated adapters are Tenable-related.

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and Axonius.

### Asset Data Validation

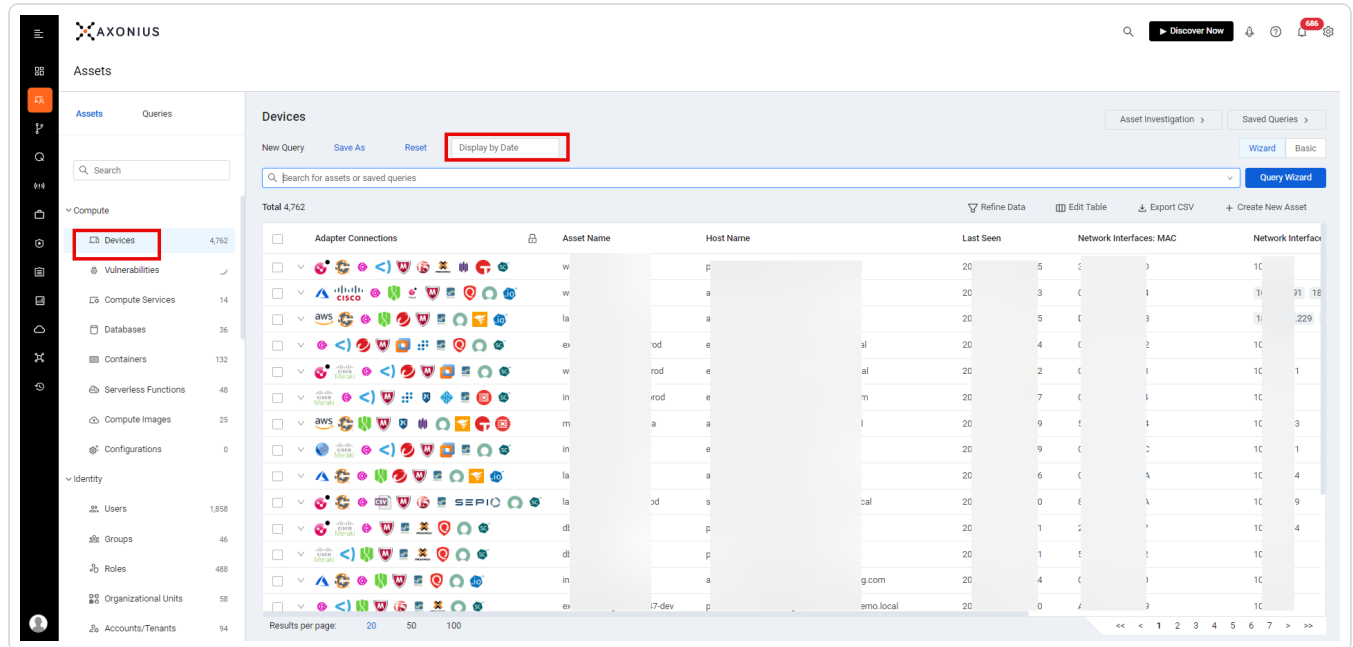
For each unique `internal_axon_id` in Axonius, the connector creates an asset in Exposure Management.

**Objective:** Ensure the number of assets (devices) in Axonius aligns with the number of devices displayed in Tenable Exposure Management.

In Axonius:



1. Navigate to the **Devices** view under the **Compute** section.
2. Apply filters to exclude archived devices (based on your configuration in [Asset Retention](#)).



In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between Axonius and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Axonius and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

If an asset meets any of the following conditions, it will not appear in Exposure Management.

- Archived based on the last observed date (field last\_seen).
- Asset isn't expected to be fetched because it is already part of [Tenable-Adapters](#).

**Tip:** To learn more on how assets are archived, see [Status Update Mechanisms](#).

## Azure Connector



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

Microsoft [Azure Virtual Machines](#) are image service instances that provide on-demand and scalable computing resources with usage-based pricing.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Azure Virtual Machines</a>
Category	Asset Inventory
Ingested data	Assets only
Ingested <a href="#">Asset Classes</a>	Device
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

### Create an Azure Application:

1. Sign in to the [Azure Portal](#) .
2. In the left navigation pane, click **Azure Active Directory**.
3. Under **Manage**, click **App registrations**.
4. Click the **+ New registration** button.



5. In the **Name** field, enter a display name for the application.
6. Under **Supported account** types, select the appropriate option based on your organization's needs.
7. (Optional) Enter a redirect URI if applicable.
8. Click **Register**.
9. After registration, make note of the following values for connector configuration:
  - **Directory (Tenant) ID**
  - **Application (Client) ID**

#### **Generate an Azure Client Secret (Service Principal Password):**

1. In the Azure Portal, navigate to **Azure Active Directory**.
2. Under **Manage**, select **App registrations**.
3. Select the application you registered for the connector.
4. In the left-hand menu, select **Certificates & secrets**.
5. Under Client secrets, click **+ New client secret**.
6. Enter a description and choose an expiration duration (e.g., 6 months, 12 months).
7. Click **Add**.

Copy the Value immediately after creation. This is the Service Principal Password. You won't be able to retrieve it later.

#### **Grant the Azure Application API permissions:**

1. In the Microsoft Azure Portal, navigate to **Subscriptions**.
2. Click the applicable subscription.
3. On the **Overview** page, click **Access Control (IAM) > Add**.
4. Click **Add role**.
5. From the **Role** drop-down, select **Reader**.



6. From the **Assign access** drop-down, select **Azure AD user, group, or service principal**
7. In the **Select** drop-down, select your Azure Application
8. Click **Save**.

**Tip:** Review these API permissions by navigating to Azure active directory > **App Registrations** > select your client application > **API Permissions**.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

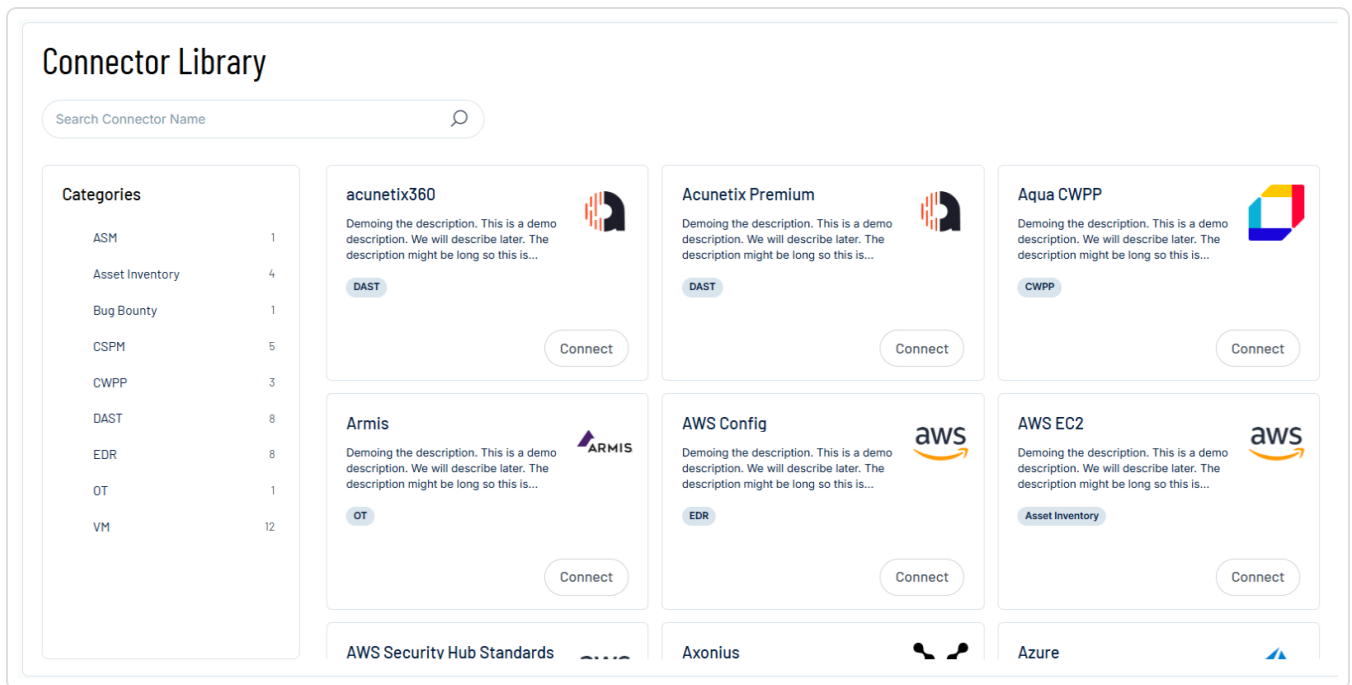
The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.





3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To set up the connector:

1. (Optional) Edit the default connector name if you need it to be more descriptive.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.


**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Tenant ID**, **Client ID**, and **Service Principal Password (Client Secret)** text boxes, enter the credentials you generated earlier.
4. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.



- **Subscriptions:** Configure to either "**Always fetch all subscription**" or select specific subscriptions to sync.

**Subscriptions**  
☐ Always fetch all subscriptions  
Select specific subscriptions to sync  

Choose 

- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) Select more statuses when detected the asset should be archived. By default, Exposure Management archives assets that return from the connector



with the state Deallocating or Deallocated .

### Asset Retention

Remove assets when their last seen date is more than  days ago

**Immediately remove assets when their status is:**

Stopping × stopped × ... ^

Q Search

☒ Stopping

☒ stopped

☒ VM deallocated

☒ Deallocating

☒ Deallocated

5 items selected.

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create** to start syncing the new connector, or **Save Changes** if editing an existing connector.
8. Allow some time for the sync to complete. Then, you can review the sync status on the **Connectors** main page or under [Connector Logs](#) on the connector's specific setup page.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Azure in Tenable Exposure Management

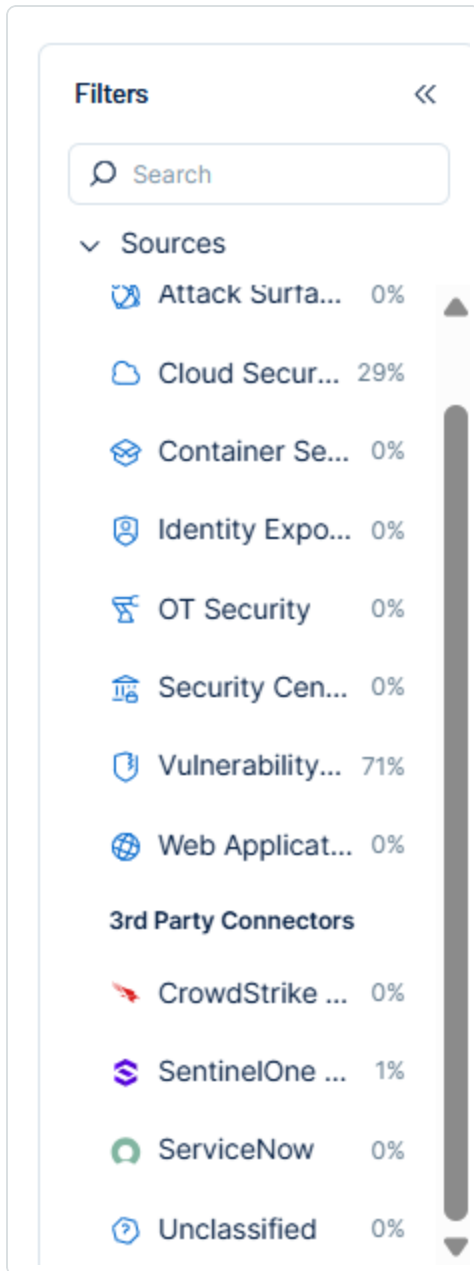
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Data Mapping



Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

<b>Tenable Exposure Management UI Field</b>	<b>Microsoft Azure Field</b>
Unique Identifier	vmId
Asset - External Identifier or Asset - Provider Identifier	vmId
Asset - Name	name
Asset - Operating Systems	properties.storageProfile.osDisk.osType
Asset - IPv4 Addresses	network_interface.data.properties.ipConfigurations.properties.privateIpAddress
Asset - IPv6 Addresses	publicIps.data.properties.ipAddress
Asset - MAC Addresses	network_interface.data.properties.macAddress
Asset - First Observation Date	instance_view.status.time



Asset - External Tags	tags
Asset Custom Attributes	os_version  instance_view.data.osName  properties.vmId  subscription_id  subscription_name

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>• Asset not seen for X days according to "Last Seen"</li><li>• Asset that returns from the connector with the state <code>Deallocating</code> or <code>Deallocated</code> is archived by default</li><li>• Optional configuration is to archive based on the states: <code>Stopping</code> or <code>stopped</code> or <code>VM deallocated</code> in the <a href="#">Data Pulling Configuration</a> on the connector setup.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria



Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	vmId

## API Endpoints in Use

API version: 2021-04-01, 2021-03-01, 2020-11-01

API URL: <https://management.azure.com>

API	Use in Tenable Exposure Management
<a href="https://login.microsoftonline.com/{{ tenant_id }}/oauth2/token">https://login.microsoftonline.com/{{ tenant_id }}/oauth2/token</a>	Authentication
<a href="https://management.azure.com/subscriptions/{{ subscription_id }}/resourcegroups?api-version=2021-04-01">https://management.azure.com/subscriptions/{{ subscription_id }}/resourcegroups?api-version=2021-04-01</a>	Resource groups
<a href="https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_name }}/providers/Microsoft.Compute/virtualMachines?api-version=2021-03-01">https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_name }}/providers/Microsoft.Compute/virtualMachines?api-version=2021-03-01</a>	Virtual Machines
<a href="https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_id }}/providers/Microsoft.Network/networkInterfaces/{{ network_interface_id }}?api-version=2020-11-01">https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_id }}/providers/Microsoft.Network/networkInterfaces/{{ network_interface_id }}?api-version=2020-11-01</a>	Network interfaces - Private IPS, MAC
<a href="https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_id }}">https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_id }}</a>	Public IPS





<code>}}/providers/Microsoft.Network/publicIPAddresses/{{ public_ip_id }}?api-version=2020-11-01</code>	
<code>https://management.azure.com/subscriptions/{{ subscription_id }}/resourceGroups/{{ group_id }}/providers/Microsoft.Compute/virtualMachines/{{ vm_id }}/instanceView?api-version=2021-03-01</code>	Virtual Machine Details

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Microsoft Azure platform.

### Asset Data Validation

**Objective:** Ensure the number of endpoints (devices) in Microsoft Azure aligns with the number of devices displayed in Tenable Exposure Management.

In Microsoft Azure:

1. Navigate to your list of **Virtual Machines**. Every Virtual Machine in Azure is ingested as a device in Exposure Management.

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
centos	Virtual machine	Vulcan-Labs-Subscription	cloud-shell-storage-weste...	West Europe	Stopped (deallocated)	Linux	Standard_B2ms	20.56.90.30	1
defender-for-cloud-vm1	Virtual machine	Vulcan-Labs-Subscription	defender-for-cloud-resou...	East US 2	Stopped (deallocated)	Linux	Standard_DS1	20.122.148.136	1
defender-for-cloud-vm2	Virtual machine	Vulcan-Labs-Subscription	defender-for-cloud-resou...	East US 2	Stopped	Windows	Standard_DS1	20.230.52.43	1
ELUS-Host01	Virtual machine	Vulcan-Labs-Subscription	sccm-lab	East US	Stopped (deallocated)	Windows	Standard_D8ds_v4	52.188.48.107	2
gatewayfw1	Virtual machine	Vulcan-Labs-Subscription	PCC-Lab-west europe	West Europe	Stopped (deallocated)	Linux	Standard_B2ms	-	1
New-Gateway	Virtual machine	Vulcan-Labs-Subscription	cloud-shell-storage-weste...	West Europe	Stopped (deallocated)	Linux	Standard_B2ms	98.71.252.60	1

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Azure and Tenable Exposure Management.



**Expected outcome:** The total numbers returned in Microsoft Azure and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

If an asset meets any of the following conditions, it will not appear in Exposure Management.

- Archived based on the last observed date.
- Archived based on the asset's status.

**Tip:** To learn more on how assets are archived, see [Status Update Mechanisms](#).

## BitSight Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[BitSight](#) helps users take a risk-based, outcome-driven approach to managing the performance of their organization's cybersecurity program through broad measurement, continuous monitoring, and detailed forecasting in an effort to measurably reduce cyber risk.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">BitSight</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices Web Applications
Integration type	UNI directional (data is transferred from the Connector to Tenable)



	Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Create a BitSight user with **Reader** permission.
- Identify your BitSight Server URL

- **Generate a BitSight API Key:**

1. In your BitSight portal, navigate to > **Settings > Account > API Token**.
2. Click **Generate New Token (API Key)**.
3. Copy the API key string carefully:

- Do not include any prefix or suffix characters (such as ' or :).
- Copy only the alphanumeric key string itself, exactly as shown in the **Current API Token** field.

**User API Token**

Current API Token: [redacted]

[Generate New Token](#) [Revoke Token](#)

You can test the API with your browser (enter your token as the username with no password), or paste the following curl command into your terminal:

```
$ curl -u [redacted] : 'https://api.bitsighttech.com/'
```

Your API token is used to authenticate to the Bitsight API. To create a new token, click Generate New Token. If you already have an API token, this will destroy your existing token and generate a new one. To delete your token without generating a new one, click Revoke Token.

Note: A user can only have one token at a time. For more information about the Bitsight API, see the [API documentation](#).

4. Save the API key in a secure location.

Use this key when setting up the BitSight connector in Exposure Management.

## Add a Connector



To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

### Connectors

Name	Connector type	Status	Last data ingestion	Created on	
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span>⋮</span>

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.

### Connector Library

#### Categories

ASM	1
Asset Inventory	4
Bug Bounty	1
CSPM	5
CWPP	3
DAST	8
EDR	8
OT	1
VM	12

acunetix360  
Demoing the description. This is a demo description. We will describe later. The description might be long so this is...  
**DAST**  
[Connect](#)

Acunetix Premium  
Demoing the description. This is a demo description. We will describe later. The description might be long so this is...  
**DAST**  
[Connect](#)

Aqua CWPP  
Demoing the description. This is a demo description. We will describe later. The description might be long so this is...  
**CWPP**  
[Connect](#)

Armis  
Demoing the description. This is a demo description. We will describe later. The description might be long so this is...  
**OT**  
[Connect](#)

AWS Config  
Demoing the description. This is a demo description. We will describe later. The description might be long so this is...  
**EDR**  
[Connect](#)

AWS EC2  
Demoing the description. This is a demo description. We will describe later. The description might be long so this is...  
**Asset Inventory**  
[Connect](#)

AWS Security Hub Standards

Axonius

Azure



3. In the search box, type the name of the connector.
4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server URL** text box, paste the url of your Bitsight server.
4. In the **API Key** text box, paste the API key you generated in Bitsight.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - You can configure how Tenable Exposure Management ingests company data from Bitsight. Two options are available:
    - To sync with specific company IDs: Click **Load Company IDs**, and then select the Bitsight company IDs you want to ingest during each sync.
    - To fetch all companies automatically: Select the **Always fetch all companies** check box. The connector will ingest data from all companies associated with your Bitsight account during each sync.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the



application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. (Optional) To exclude vulnerabilities based on lifetime-expired risk vectors, select the **Map lifetime expired risk vector vulnerabilities as Ignored** check box.
7. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

8. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

9. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
10. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

BitSight in Tenable Exposure Management

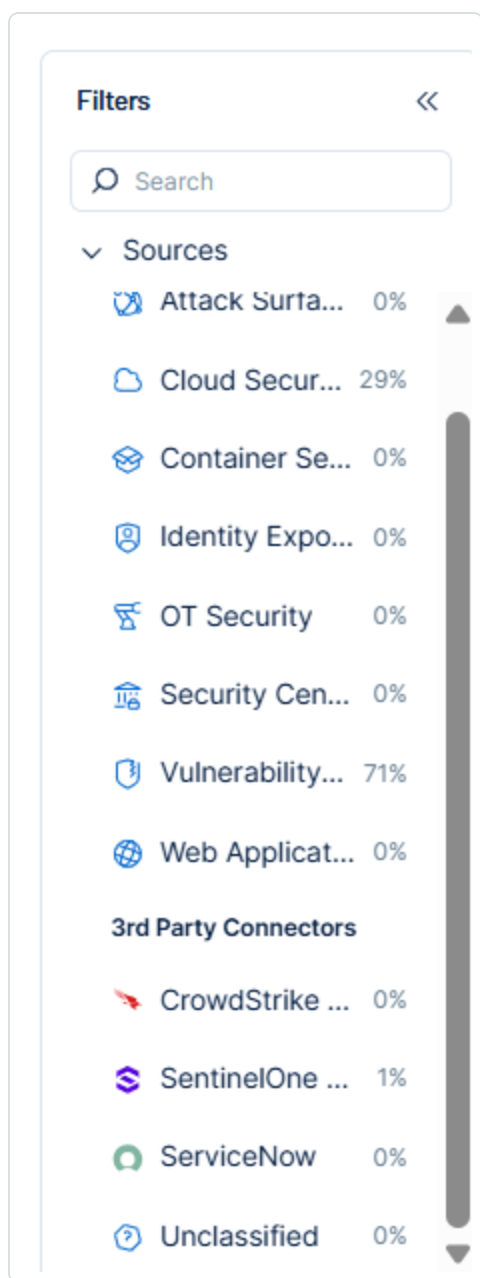


## Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Locate Connector Weaknesses in Tenable Exposure Management

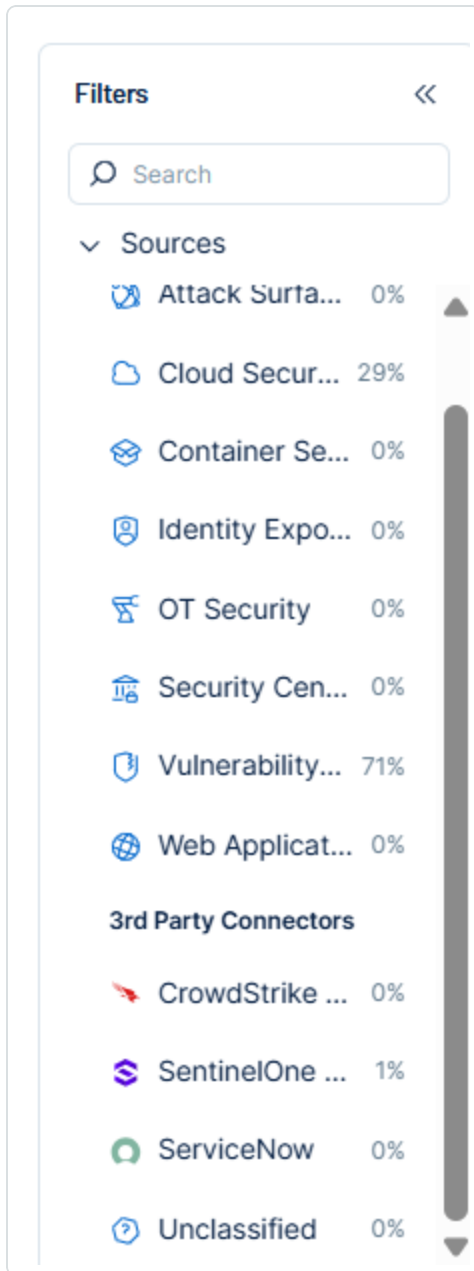
As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:





1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

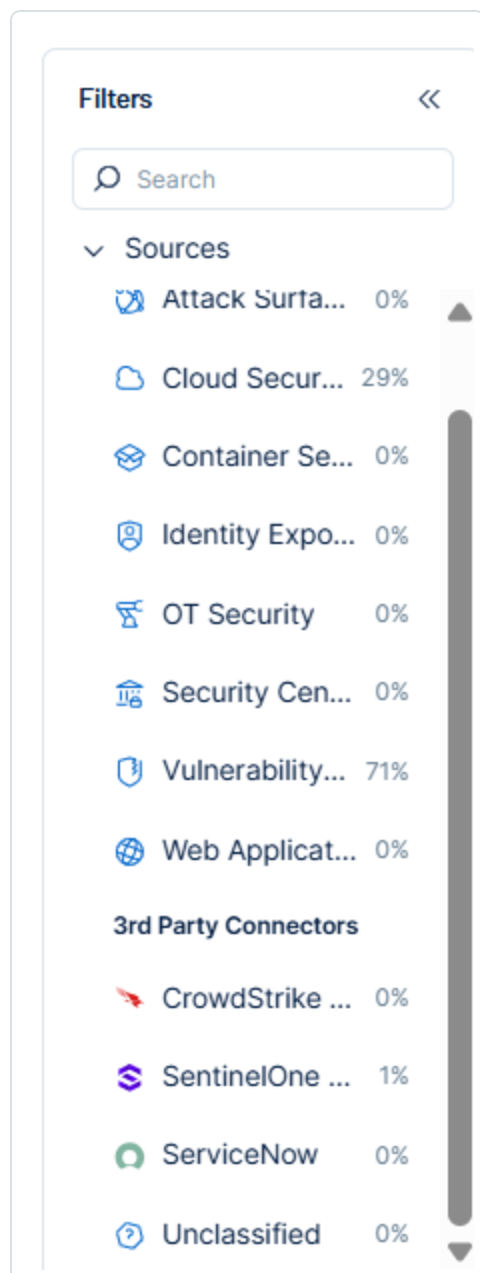
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	BitSight Field
Unique Identifier	asset
Asset - Name	asset
Asset - Operating Systems	products.product (if type = operating system)
Asset - IPv4 Addresses	ip_addresses
Asset - IPv6 Addresses	
Asset - External Tags	tags
Asset Custom Attributes	products.version

## Device Finding Mapping

Tenable Exposure Management UI Field	BitSight Field
Unique Identifier	evidence_key
Finding Name	help_text/message
Severity Driver	severity
Description	help_text
Port	dest_port



First Seen	first_seen
Last seen (Observed)	last_seen
Finding Custom Attributes	temporary_id evidence_key remaining_decay grade impacts_risk_vector_details risk_vector_label risk_category severity_category

### Web Application Mapping

Tenable Exposure Management Value	BitSight Field
Unique Identifier	asset
Asset - Name	asset
Asset - Webapp Homepage Screenshot Url	asset (if asset_type = Domain)
Asset - External Tags	tags

### Web Application Finding Mapping

Tenable Exposure Management UI Field	BitSight Field
Unique Identifier	evidence_key
Finding Name	help_text/message
Severity Driver	severity
Description	help_text



First Seen	<code>first_seen</code>
Last seen (Observed)	<code>last_seen</code>
Finding Custom Attributes	<code>temporary_id</code> <code>evidence_key</code> <code>remaining_decay</code> <code>grade</code> <code>impacts_risk_vector_details</code> <code>risk_vector_label</code> <code>risk_category</code> <code>severity_category</code>

### Finding Status Mapping

Tenable Exposure Management Status	BitSight Status
Active	All other statuses, including: <code>lifetime_expired_ignored=True</code> <code>impacts_risk_vector_details=lifetime_expired</code> <code>risk accepted</code>
Fixed	<code>resolved</code> <code>remaining_decay=0</code>

**Note:**For BitSight, Exposure Management bases the finding status on the `last_remediation_status_label` field.

### Finding Severity Mapping

Tenable Exposure Management Severity	BitSight Score
--------------------------------------	----------------



Critical	9-10
High	7-8
Medium	4-6
Low	1-3

**Note:** For BitSight, Exposure Management bases the finding score on the `severity` field.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <code>last_remediation_status_label = resolved</code> OR <code>remaining_decay=0</code> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).



The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	asset
Detection	help_text/message
Finding	evidence_key
Solution	remediation_tip

## API Endpoints in Use

API version: v2

API	Use in Tenable Exposure Management	Required Permissions
/ratings/v1/companies	Get companies Ids	Reader
/ratings/v1/companies/{{ company_guid }}/assets	Assets	Reader
/ratings/v1/companies"/{{ company_guid }}/findings	Findings	Reader

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the BitSight platform.

### Asset Data Validation

**Objective:** Ensure that the number of assets in BitSight aligns with the number of assets displayed in Exposure Management.

In BitSight:

1. Navigate to the **Findings** page.
2. Click on a finding to open its **Details** tab.



### 3. Review the **Asset** field:

- If an asset is listed, this is the asset that will appear in Exposure Management.
- If no asset is listed, the finding is considered assetless and will not appear in Exposure Management.

### In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between BitSight and Tenable Exposure Management.

**Expected outcome:** Only findings that are tied to an asset in BitSight will be represented as assets in Exposure Management. Asset counts may differ if BitSight findings are not associated with an asset.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on its last observed date (`last_seen` field).
- The asset was archived because it did not return in the connector's last sync.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

### Finding Data Validation

**Objective:** Ensure that the number of findings in BitSight aligns with the number of findings in Exposure Management.

### In BitSight:

1. Navigate to the **Findings** page.
  - Each finding includes a **Risk Vector**, **Finding Identifier**, and **Details**.
  - These parameters are used to determine uniqueness. Each unique finding should be reflected in Exposure Management.

### In Tenable Exposure Management:





1. [Locate your connector findings.](#)
2. Compare the total number of findings between BitSight and Tenable Exposure Management.

Findings are considered unique based on the combination of:

- Risk Vector
- Finding Identifier
- Details (mapped from BitSight remediation name)

**Expected outcome:**Exposure Management may display fewer findings if multiple BitSight entries share the same unique combination, or if findings are not tied to an asset.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## BlackDuck (formerly WhiteHat) Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[BlackDuck Continuous Dynamic \(formerly WhiteHat™ Dynamic\)](#) rapidly and accurately finds vulnerabilities in websites and applications with the scale and agility you need to identify security risks across your entire application portfolio.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
---------	-------------



Supported products	<a href="#">BlackDuck Continuous Dynamic</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Applications
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Identify your WhiteHat API (BlackDuck Continuous Dynamic) URL (e.g., <https://sentinel.whitehatsec.com/api>)
- **Generate a WhiteHat (BlackDuck Continuous Dynamic) API Key:**
  1. Navigate to the **BlackDuck Continuous Dynamic** Platform.
  2. In the **My Profile** page, select **API Key**.
  3. Type your password into the **Verify Password** text field.
  4. Click **Authenticate** to display your key. If you have never requested your API key before, a key will be generated for you.

**Tip:** For more information, see the [WhiteHat Documentation](#).

## Add a Connector

To add a new connector:



1. In the left navigation menu, click **Connectors**.























The **Connectors** page appears.

Connectors

Add new connector

Search Connector Name

Select

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> 
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> 
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> 
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> 
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> 
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> 
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> 

2. In the upper-right corner, click [+ Add new connector](#).

The **Connector Library** appears.

### Connector Library

Search Connector Name

#### Categories

ASM	1
Asset Inventory	4
Bug Bounty	1
CSPM	5
CWPP	3
DAST	8
EDR	8
OT	1
VM	12

acunetix360

Demoting the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoting the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoting the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoting the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoting the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoting the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.



The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Url** section, type your Whitehat (BlackDuck Continuous Dynamic) API base URL.
4. In the **API Key** text box, paste the API key you generated in Whitehat (BlackDuck Continuous Dynamic).
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

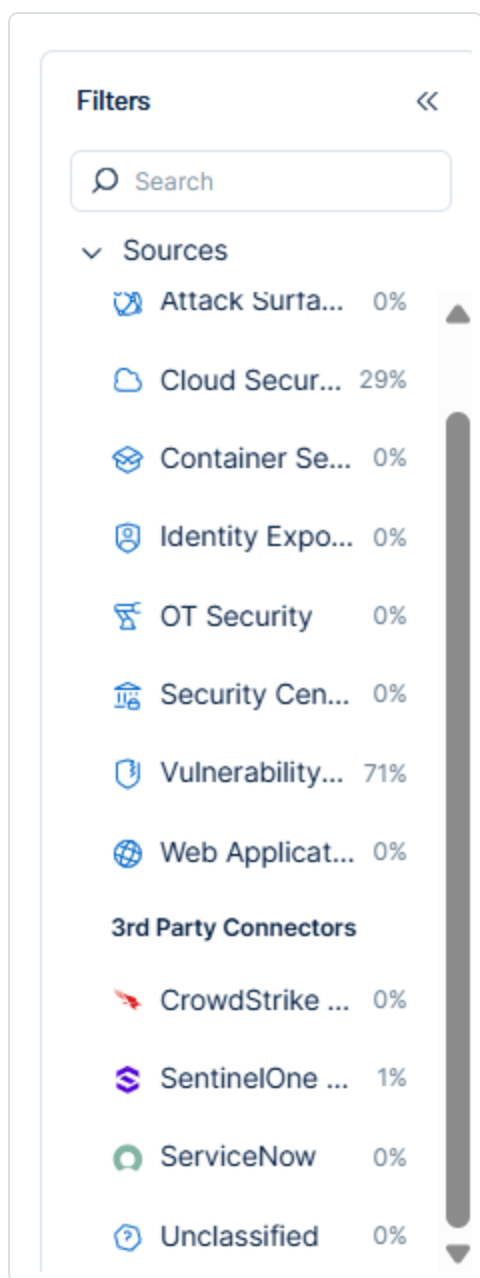
## BlackDuck Continuous Dynamic in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

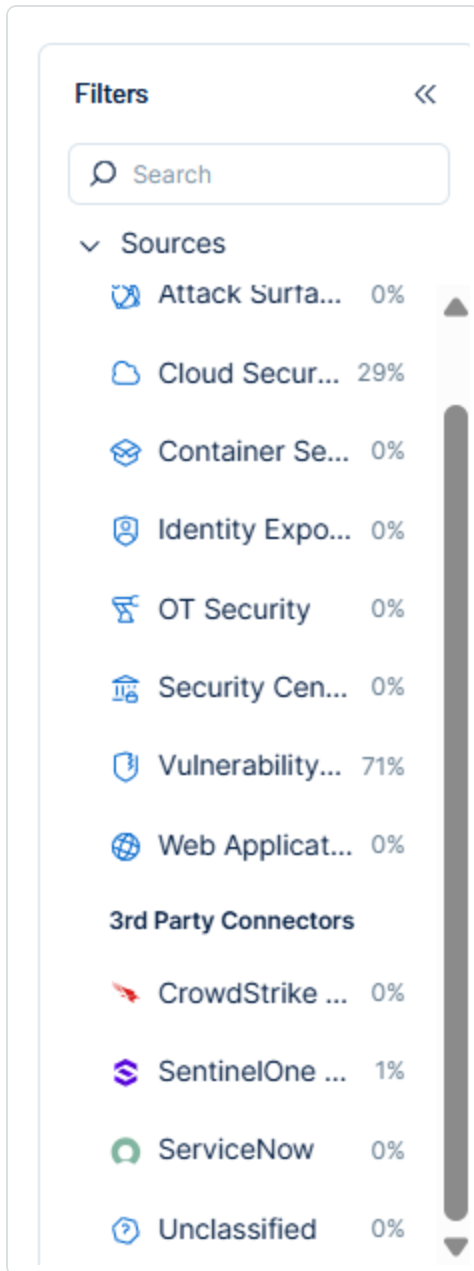
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

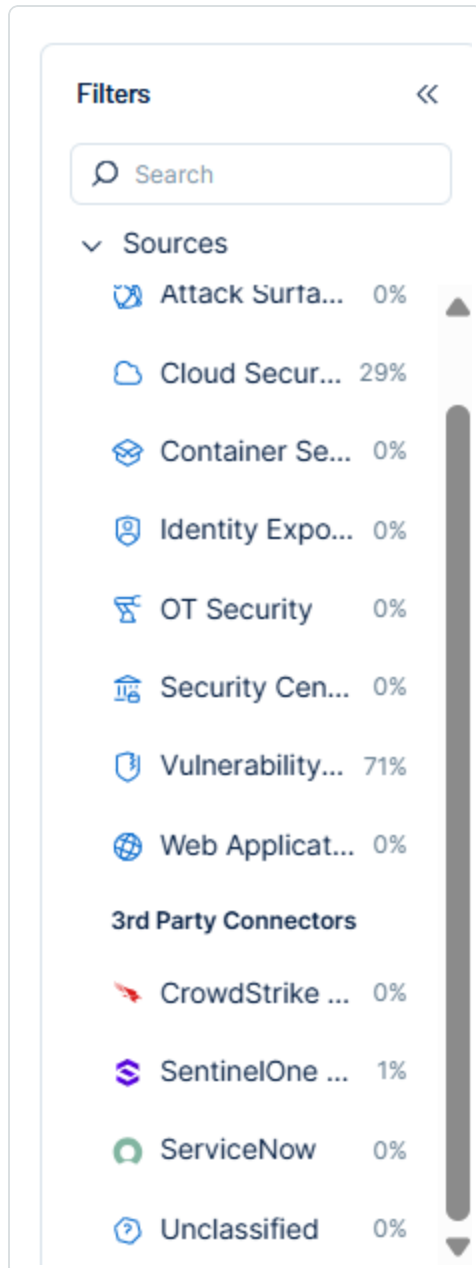
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings







The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management Value	WhiteHat (BlackDuck Continuous Dynamic) Value
Unique Identifier	id
Asset - Name	label
Asset - First Observation Date	first_completed_scan.timestamp
Asset - Last Observed At	last_completed_scan.timestamp
Asset - Webapp Homepage Screenshot Url	allowed_hosts[0.hostname
Asset - External Tags	tags
Asset Custom Attributes	id client_id organization description allowed_hosts asset_owner_name wsi_global_rank wsi_score



	scan_status
	asset_phase groups

## Finding Mapping

Tenable Exposure Management UI Field	WhiteHat (BlackDuck Continuous Dynamic) Field
Unique Identifier	id
Finding Name	class
Severity Driver	cvss_v3_score or cvss_v3_score_rating
Description	description.description
First Seen	opened
Last seen (Observed)	modified
Finding Custom Attributes	attack_vectors description_prepend whitehat link: <a href="https://source.whitehatsec.com/asset-management/site-summary/{{ site }}/findings/{{ id }}">https://source.whitehatsec.com/asset-management/site-summary/{{ site }}/findings/{{ id }}</a> impact reason risk cvss_v3_score_rating cvss_v3_vector

## Finding Status Mapping

Tenable Exposure Management Status	WhiteHat (BlackDuck Continuous Dynamic) Status
------------------------------------	--



Active	All other statuses, including: out of scope, accepted, invalid, and mitigated
Fixed	closed

**Note:**For WhiteHat (BlackDuck Continuous Dynamic), Exposure Management uses the status field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	WhiteHat (BlackDuck Continuous Dynamic) Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:**For WhiteHat (BlackDuck Continuous Dynamic), Exposure Management uses the cvss\_v3\_score field to determine severity. If cvss\_v3\_score is not available, Exposure Management uses the cvss\_v3\_score\_rating field from the connector, if provided.

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.



**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Finding	id
Detection	class

### Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <code>closed</code> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

### API Endpoints in Use

API	Use in Tenable Exposure Management
{{{ api_url }}}/site	Assets



{{{ api\_url }}}/vuln/stats

Findings

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the BlackDuck Continuous Dynamic platform.

### Asset Data Validation

**Objective:** Ensure the number of assets in BlackDuck Continuous Dynamic aligns with the number of assets displayed in Tenable Exposure Management.

In BlackDuck Continuous Dynamic:

1. Navigate to the **Assets** section.
2. Set the assets filter to:
  - Asset type: Site

The screenshot shows the Tenable Asset Management interface. The top navigation bar includes tabs for Summary, Assets, Components, Findings, and Reports. The 'Assets' tab is selected. Below the navigation bar, there's a section titled 'Asset Management' with an 'Export CSV' link. A table lists assets with columns: Name, Scan Setup Issues, Scan Status, Asset Status, Asset Phase, and Asset Type. The table contains three rows of assets. To the right of the table is a sidebar with a 'Filter' button and a 'Frequently Used' section. The 'Filter' button is highlighted.

Name	Scan Setup Issues	Scan Status	Asset Status	Asset Phase	Asset Type
DVWA	Missing BLA Credentials	BDCD Updating Configuration	Active	--	Site
WebGoat Site -DAST	--	Scan Running	Active	--	Site
WH Sandbox App	Needs Codebase Configure Satellite Appliance Unreachable	BDCD Updating Configuration	Active	--	Application

3. Click **Filter** to apply.

These site assets correspond to the filtered BlackDuck Continuous Dynamic DAST assets in Exposure Management.

In Tenable Exposure Management:



1. [Locate your connector assets.](#)
2. Compare the total number of assets between BlackDuck Continuous Dynamic DAST and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in BlackDuck Continuous Dynamic and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived based on the last observed date (last seen).
- Archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the total number of findings between BlackDuck Continuous Dynamic and Exposure Management is consistent.

In BlackDuck Continuous Dynamic:

1. Navigate to the **Findings** section.
2. Set the findings filter to:
  - Asset type: Site
  - Vulnerability Status: Open
3. Click **Filter** to apply.
4. Scroll to the bottom of the list to view the total number of open findings.

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between BlackDuck Continuous Dynamic and Tenable Exposure Management.



**Expected outcome:** Exposure Management only displays findings that are in "Open" status and tied to an asset of type "Site" in WhiteHat (BlackDuck Continuous Dynamic). Counts may differ if filters are misapplied or if related assets are missing. If filtered correctly in both platforms, the total number returned in WhiteHat (BlackDuck Continuous Dynamic) and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## Cortex XDR Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Cortex XDR](#) is a detection and response app that natively integrates network, endpoint, and cloud data to stop sophisticated attacks. It accurately detects threats with behavioral analytics and reveals the root cause to speed up investigations.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Cortex XDR</a>
Category	Endpoint Security
Ingested data	Assets and Findings



Ingested <a href="#">Asset Classes</a>	Devices
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Have Cortex XDR Pro license per endpoint
- **Generate Cortex XDR API Key, ID, and FQDN:**

Follow the instructions at [Get Started with Cortex XDR APIs](#) to get your:

1. Cortex XDR API Key
2. Cortex XDR API Key ID
3. FQDN

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.


















Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

DAST

Connect

Acunetix Premium

DAST

Connect

Aqua CWPP

CWPP

Connect

Armis

OT

Connect

AWS Config

EDR

Connect

AWS EC2

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

- 493 -



To configure the connector:

5. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
6. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

7. Paste the **FQDN**, **API Key**, and **API ID** values you generated in Cortex XDR.
8. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- For the **Immediately remove assets when their status is** option, choose to automatically remove assets that reach a certain asset status, for example, **LOST**.
9. Click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your **Cortex XDR** instance.
    - In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
      - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
      - If the connectivity test fails, an error message with details about the issue



appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ **Failed tests** 1 out of 4 integration tests failed

✔ **Successful tests** 3 out of 4 integration tests succeeded

10. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

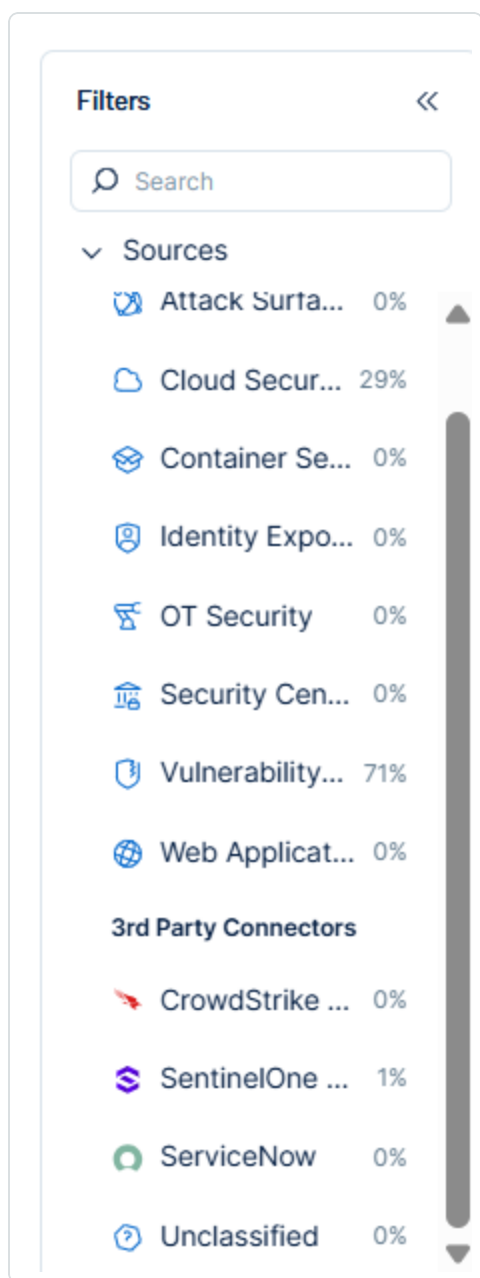
11. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
12. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

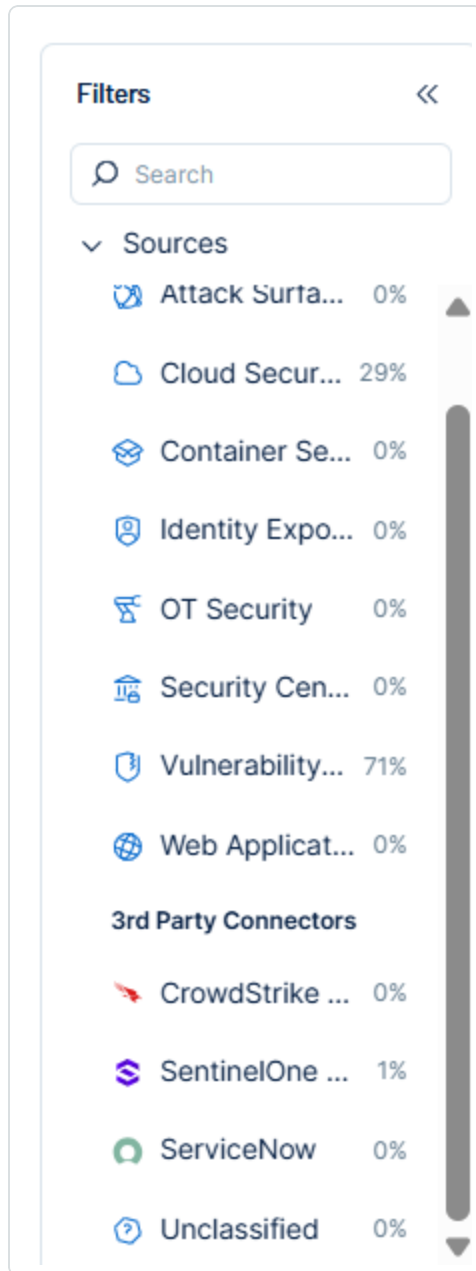
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

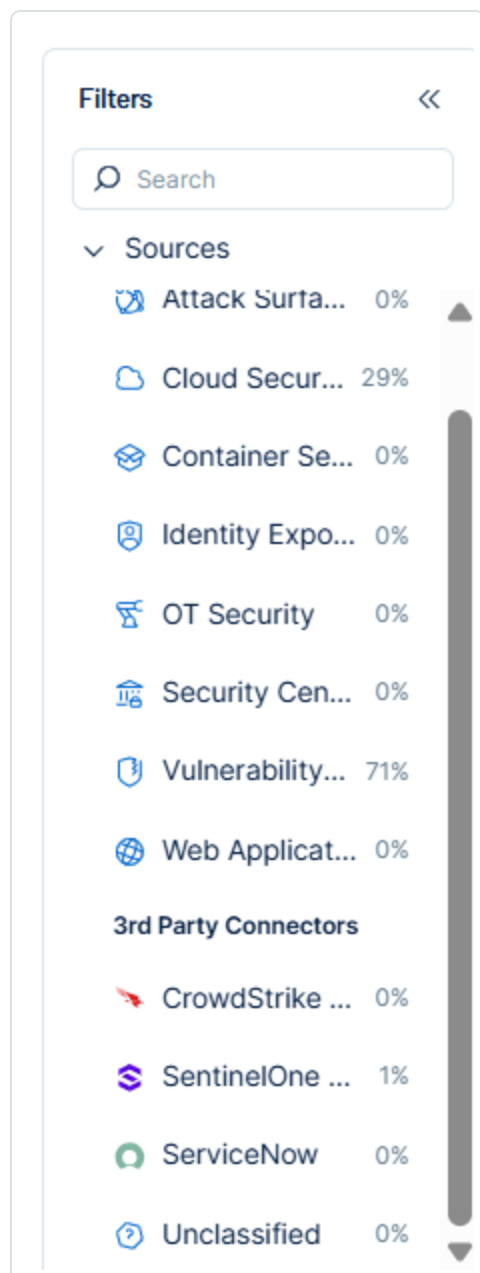
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Cortex XDR Field
Unique Identifier	endpoint_id
Asset - External Identifier or Asset - Provider Identifier	endpoint_id
Asset - Name	endpoint_name
Asset - IPv4 Addresses Asset - IPv6 Addresses	id
Asset - Operating Systems	operating_system
Asset - Host Fully Qualified DNS	domain
Asset - MAC Addresses	mac_address
Asset - First Observation Date	first_seen
Asset - Last Observed At	last_seen
Asset - External Tags	tags
Asset Custom Attributes	os_version os_type users

## Finding Mapping



Tenable Exposure Management UI Field	Cortex XDR Field
Unique Identifier	endpoint_name + cve_id
Finding Name	name
CVEs	name
Severity Driver	severity_score
Description	description

### Finding Severity Mapping

Tenable Exposure Management Severity	Cortex XDR Score
Critical	<b>Severity:</b> Critical
High	<b>Severity:</b> High
Medium	<b>Severity:</b> Medium
Low	<b>Severity:</b> Low

**Note:** For Cortex XDR, Tenable uses the `severity_score` field to determine severity.

### Finding Status Mapping

Tenable Exposure Management Status	Cortex XDR Status
Active	vulnerable

### Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
------------------------------------	-------------------





Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a>]</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	endpoint_id
Finding	endpoint_name + cve_id

## API Endpoints in Use

API version: v1.0

		Required Permissions
<a href="https://api-amadeus-sas.xdr.eu.paloaltonetworks.com/public_api/v1/endpoints/get_endpoint">https://api-amadeus-sas.xdr.eu.paloaltonetworks.com/public_api/v1/endpoints/get_endpoint</a>		Cortex XDR Pro license per endpoint
<a href="https://api-amadeus-">https://api-amadeus-</a>	Detections	Cortex XDR Pro



sas.xdr.eu.paloaltonetworks.com/public_ api/v1/xql/start_xql_query		license per endpoint
---	--	-------------------------

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Endpoint Sync Limitation

Currently, the integration does not support environments with more than 1,000 endpoints.

If a sync is attempted in an environment exceeding this limit, the process will fail. A corresponding error message will appear in the logs, indicating that the endpoint count exceeded the supported threshold.

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the **CONNECTORX** platform.

### Asset Data Validation

**Objective:** Ensure that the number of endpoints in Cortex XDR matches the number of devices displayed in Exposure Management.

In Cortex XDR:



1. Navigate to the **All Endpoints** view.

Endpoint Name	Endpoint Type	Endpoint Status	Platform	Operating System	Agent Version	IP Address	IPv6 Address
3	Workstation	Disconnected	Windows	Windows 11	38	233	200
3	Workstation	Disconnected	Windows	Windows 11	15	1231	
21	Workstation	Disconnected	Windows	Windows 10	54	76.1	
307-107	Workstation	Connected	Windows	Windows 10	37	1.126	
306-16	Workstation	Disconnected	Windows	Windows 10	37	1.99	
212-7	Workstation	Disconnected	Windows	Windows 10	38	1.123	
306-52	Workstation	Connected	Windows	Windows 10	54	1.111	
306-51	Workstation	Connected	Windows	Windows 10	54	1.57	
17	Workstation	Disconnected	Windows	Windows 11	1	151	fc0c
2	Workstation	Disconnected	Windows	Windows 11	38	204	280
12	Workstation	Disconnected	Windows	Windows 11	37	170	fc0c
15	Workstation	Disconnected	Windows	Windows 10	15	243	2a0
15	Workstation	Disconnected	Windows	Windows 11	15	1214	

2. Review the total number of endpoints displayed at the top of the All Endpoints page.

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Cortex XDR and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Cortex XDR and Exposure Management should match.

**Important!** Cortex XDR may include multiple endpoints with the same name. These are treated as distinct assets and will appear as separate entries in Exposure Management.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived because it did not return in the connector's most recent sync.
- The asset was archived based on its **Last Seen** timestamp, according to the configured retention period.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the number of active findings in Cortex XDR matches the findings displayed in Exposure Management.



In Cortex XDR:

1. Navigate to **Assets > Vulnerability Assessment**.

Host Inventory	DRE	PLATFORMS	AFFECTED ENDPOINTS COUNT	AFFECTED ENDPOINTS	LAST MODIFIED	COMMENT	PUBLICATION DATE
Applications		Windows	4	D02 + 3 More	Jan 1st 2025 16:17:22		Mar 12th 2024 19:15:00
Daemons		Windows	1	D02	Jan 1st 2025 16:16:51		Jul 15th 2020 02:15:00
Disks		Windows	4	D02 + 3 More	Jan 1st 2025 16:17:22		Jan 9th 2024 20:15:00
Drivers		Windows	1	D02	Jan 1st 2025 16:16:56		Dec 10th 2020 02:15:00
Extensions		Windows	1	D02	Jan 1st 2025 16:13:31		Jul 13th 2022 02:15:00
Mounts		Windows	1	D02	Jan 1st 2025 16:19:15		Aug 12th 2021 21:15:00
Services		Windows	2	D02 + 1 More	Jan 1st 2025 16:15:34		Oct 10th 2023 21:15:00
Shares		Windows	1	D02	Jan 1st 2025 16:16:51		Jul 15th 2020 02:15:00
System Information		Windows	1	D02	Jan 1st 2025 16:14:13		Apr 9th 2019 03:29:00
Users		Windows	1	D02	Jan 1st 2025 16:16:46		Sep 11th 2020 20:15:00
Users To Groups		Windows	1	D02	Jan 1st 2025 16:16:50		Jul 15th 2020 02:15:00
		Windows	1	D02	Jan 1st 2025 16:19:38		Nov 10th 2021 03:19:00
		Windows	1	D02	Jan 1st 2025 16:14:21		Dec 11th 2019 00:15:00

2. Each row represents a vulnerability assessment.
3. Use the **Affected Endpoints** field to view the number of findings associated with each vulnerability.
4. To validate the total number of findings, sum the **Affected Endpoints** values across all assessments. This total should match the number of active findings in Exposure Management.

In Tenable Exposure Management:

1. [Locate your connector findings](#).
2. Compare the total number of findings between Cortex XDR and Tenable Exposure Management.

**Expected outcome:** The total number of active findings in Tenable Exposure Management should match the combined count of affected endpoints across all vulnerability assessments in Cortex XDR.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen
- The finding no longer appears because its related asset was archived.



**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## CrowdStrike Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[CrowdStrike](#) is cloud-delivered endpoint protection. CrowdStrike Falcon unifies next-generation antivirus, endpoint detection and response (EDR), and a 24/7 threat-hunting service — all delivered via a single lightweight agent.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Tenable Exposure Management ingests CrowdStrike devices and vulnerabilities through API.

Details	Description
Supported products	CrowdStrike Falcon
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Device
Integration type	UNI directional (data is transferred from the connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

### Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:



- **Generate CrowdStrike API and Secret Keys:**

Some CrowdStrike accounts are divided into multiple customers, with multiple CIDs, each customer has its own CID. The CIDs are arranged in a parent/child (member) hierarchy. A parent CID has access to all of the account's hosts, including those associated with its child CIDs. Only the child CID has access to its own host groups and vulnerabilities.

**Note:** Ensure you create the API Client using the appropriate user.

1. Navigate to the CrowdStrike console.
2. Click **Menu > Support and resources**.
3. In the **Support and resources** menu, select **API clients and keys**.
4. In the upper-right corner of the page, click **Add new API client**.
5. In the **Client name and description** section, type the appropriate information.
6. In the **API Scopes** section, configure the following permissions (if available):
  - **Hosts:** Read
  - **Hosts groups:** Read
  - **Spotlight vulnerabilities:** (read)
7. Click **Add**.

Crowdstrike generates the API client information.

8. Copy and save the **CLIENT ID**, **SECRET** and **BASE URL**.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

Configure the Connector

- 507 -



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Url** section, select the radio button for the URL that matches your Base URL.
  - **EU\_1** – api.eu-1.crowdstrike.com
  - **US\_1** – api.crowdstrike.com
  - **US\_2** – api.us-2.crowdstrike.com
  - **US\_GOV\_1** – api.laggar.gcw.crowdstrike.com
4. In the **Client ID** and **Client Secret** text boxes, enter the credentials you generated earlier.
5. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.
  - From the **Crowdstrike product type fetching** drop-down, select the product type you want to fetch data from.
  - For the "**Fetch Spotlight vulnerability information**" checkbox, consider the following:
    - If your CrowdStrike subscription does not include Spotlight, make sure to clear this checkbox. Enabling it without Spotlight access may result in incomplete or failed data ingestion.
    - If you own both EDR and Spotlight, leave the checkbox selected to include vulnerability data from Spotlight.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the





application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Crowdstrike in Tenable Exposure Management

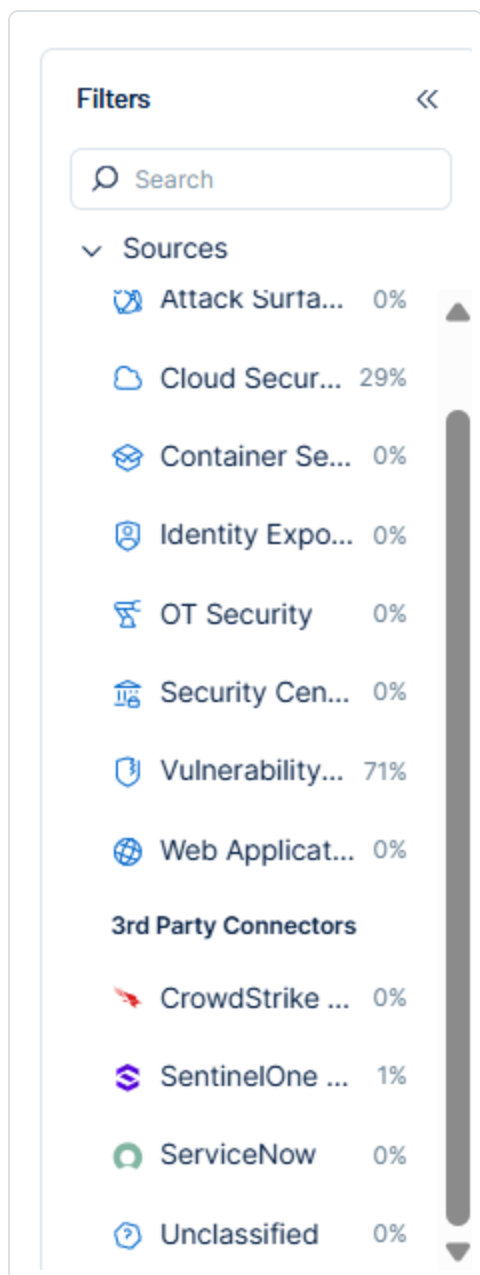
## Locate Connector Assets in Tenable Exposure Management



As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.





The asset list updates to show only assets from the selected connector.

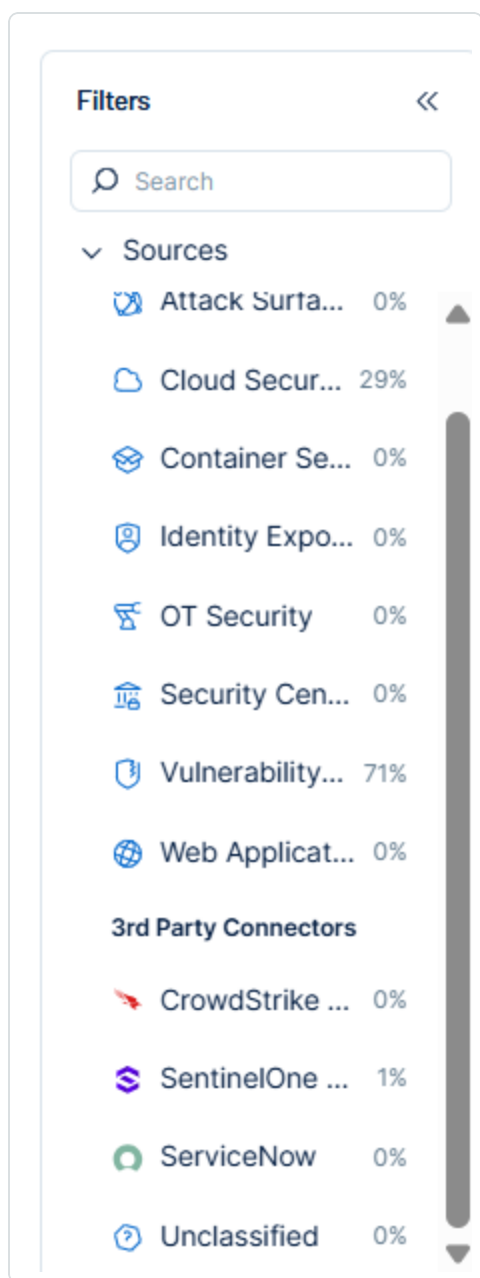
3. Click on any asset to view [Asset Details](#).

## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:

1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

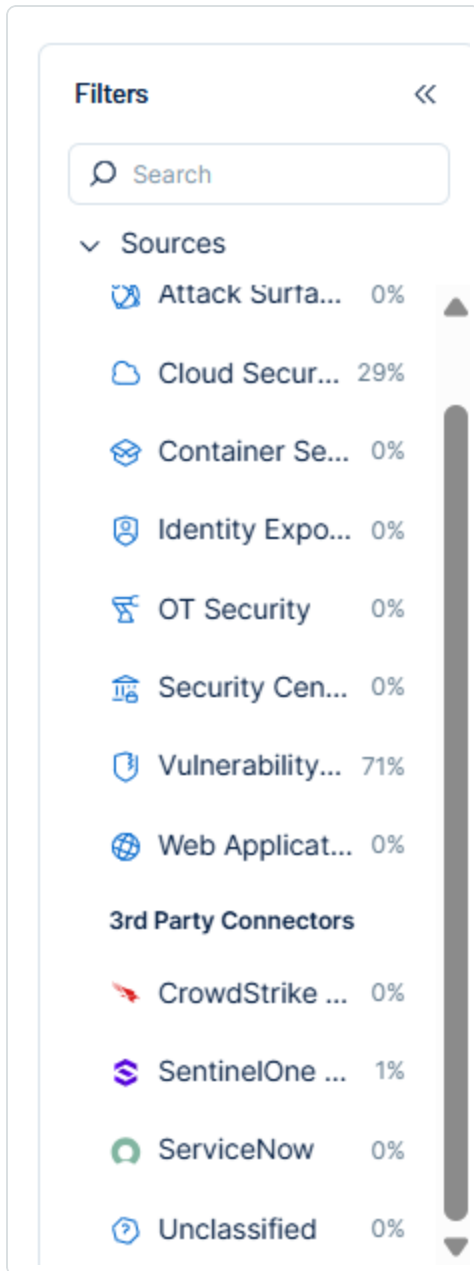
## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:



1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings



The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping



Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	CrowdStrike Field
Unique Identifier	device_id
Asset - External Identifier or Asset - Provider Identifier	instance_id
Asset - Name	hostname or ip
Class	Host
Asset - IPv4 Addresses	external_ip
Asset - IPv6 Addresses	local_ip
Asset - First Observation Date	first_seen
Asset - Last Observed At	last_seen
Asset - MAC Addresses	mac_address
Asset - External Tags	tags cid product_type_desc machine_domain
Asset Custom Attributes	major_version.minor_version containment_status device_id os_build kernel_version



## Finding Mapping

Tenable Exposure Management UI Field	CrowdStrike Field
Unique Identifier	<code>id</code>
Finding Name	<code>cve.id</code>
CVEs	<code>cve.id</code>
CWEs	<code>cve.cwe</code>
Severity Driver	<code>cve.base_score</code> or <code>cve.severity</code>
Description	<code>cve.description</code>
Finding Custom Attributes	<code>cve.vector</code> <code>cve.expirt_rating</code> <code>cid</code> <code>aid</code> <code>id</code> <code>cve.severity</code> <code>cve.references</code> <code>cve.vendor_advisory</code>
First Seen	<code>created_timestamp</code>
Last seen (Observed)	<code>updated_timestamp</code>

## Finding Severity Mapping

Tenable Exposure Management Severity	Crowdstrike Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9



	<b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> Information

**Note:** For CrowdStrike, Tenable uses the `cve.base_score` field to determine severity. If `cve.base_score` is not available, Tenable uses the `cve.severity` field from the connector, if provided.

## Finding Status Mapping

Tenable Exposure Management Status	CrowdStrike Status
Active	open reopen
Fixed	closed is_suppressed expired

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and</li></ul>





	isn't returned on the next connector's sync.
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding status changes to <b>closed</b> on the vendor's side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** To learn more about data deduplication and uniqueness criteria, See [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	device_id
Detection	<a href="#">SecAlerts</a>
Finding	id

## API Endpoints in Use

API	Use in Tenable Exposure Management	Permissions required
<a href="https://{api_url}/oauth2/token">https://{api_url}/oauth2/token</a>	Generate access tokens for running other APIs	None
<a href="https://{api_url}/devices/queries/devices/v1">https://{api_url}/devices/queries/devices/v1</a>	Collect host IDs for running	Hosts (read)



	other APIs	
<code>https://{api_url}/devices/entities/devices/v2</code>	Assets (Devices)	Hosts (read)
<code>https://{api_url}/devices/combined/host-groups/v1</code>	Asset enrichment	Hosts groups (read)
<code>https://{api_url}/devices/queries/host-group-members/v1</code>	Asset enrichment	Hosts groups (read)
<code>https://{api_url}/spotlight/combined/vulnerabilities/v1</code>	Detections and solutions	Spotlight vulnerabilities (read)

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the CrowdStrike platform.

### Asset Data Validation

**Objective:** Ensure the number of endpoints (devices) in CrowdStrike aligns with the number of devices displayed in Tenable Exposure Management. Every managed asset in Crowdstrike should appear as a device in Exposure Management.

In CrowdStrike:



1. Navigate to the **Managed Assets** tab.

Note the number of assets.

The screenshot shows the Tenable Managed Assets dashboard. At the top, there's a navigation bar with tabs for 'Assets dashboards', 'Managed assets' (selected), 'Unmanaged assets', 'Unsupported assets', and 'System insights'. Below the navigation bar, there's a search bar and a filter bar. The filter bar shows '3 items' and various filter options like 'Hostname', 'Sensor ID', 'IP address history', 'MAC address', 'Organizational unit', 'Tags', 'Domain', 'Platform', 'OS version', 'Device type', and 'Internet exposure'. Below the filter bar, there's a table with columns: Hostname, Sensor ID, IP address history, MAC address, Organizational unit, Domain, Platform, OS version, Internet exposure, Last seen, and Actions. The table contains three rows of asset data.

Hostname	Sensor ID	IP address history	MAC address	Organizational unit	Domain	Platform	OS version	Internet exposure	Last seen	Actions
CrowdStrike16	0...	10.6.0.4	00-2...	C	--	Windows	Windows Server 2016	(Unknown)	Feb. 16, 2023 15:0..	⋮
DESKTOP-FIO6ILE	c...	192.168.69.84	9C-B...	35	--	Windows	Windows 10	(Unknown)	Jan. 23, 2023 17:0..	⋮
lp-172-31-42-71us-ea...	d...	172.31.42.71	0A-5...	A	--	Linux	CentOS 7.7	(Unknown)	Feb. 16, 2023 14:0..	⋮

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between CrowdStrike and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in CrowdStrike and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived because it did not return in the connector's last sync.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

Finding Data Validation

**Objective:** Ensure the number of vulnerabilities in CrowdStrike aligns with the number of findings in Tenable Exposure Management.

In CrowdStrike:



## 1. Navigate to **Vulnerabilities**.

Note the number of vulnerabilities.

ExPRT rating	Severity	Status	Opened within	Vendor & product	Last seen within	Exploit status
Critical	High	Open	Last 30 days Last 60 days Last 90 days	Microsoft Windows 10 Microsoft Windows Server 2016	Last 3 days Last week Last 14 days Last 30 days Last 45 days	Actively used (critical) Easily accessible (high, critical) Available (medium, high, critical) Unproven

ExPRT rating	Severity	CVE ID	Products	Vulnerabilities	Exploit status	Remediations	Open	Actions
Critical	High	CVE-2013-3900	2	2	Actively used (critical)	2	2	[Icons]

In Tenable Exposure Management:

1. [Locate your connector findings](#).
2. Compare the total number of findings between CrowdStrike and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in CrowdStrike and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## CyCognito Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).



The [CyCognito platform](#) discovers and tests all assets discoverable via the internet. This process finds previously unknown assets unmonitored and exposed to attack. The platform continuously monitors and tests all assets associated with an organization.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">CyCognito</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices Web Applications
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Create a CyCognito user with the necessary permissions to generate and manage API keys within the CyCognito platform.
- Identify your CyCognito platform URL.
- **Generate a CyCognito API Key:**
  1. In your CyCognito Platform, navigate to **Workflow & Integration**.
  2. Click **API Key Management**.



3. Type a **Key Name**.

A dark-themed dialog box titled "Generate new API key". It contains a "Key name" label above a text input field. Below this is a "Key access" section with two radio buttons: "Read only" (selected) and "Read and write". At the bottom left is a "Set expiration" label with a toggle switch set to "OFF". At the bottom right are two buttons: "Cancel" and "Create".

4. Click **Create**.

5. Save the resulting API key for later use within in Tenable Exposure Management.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

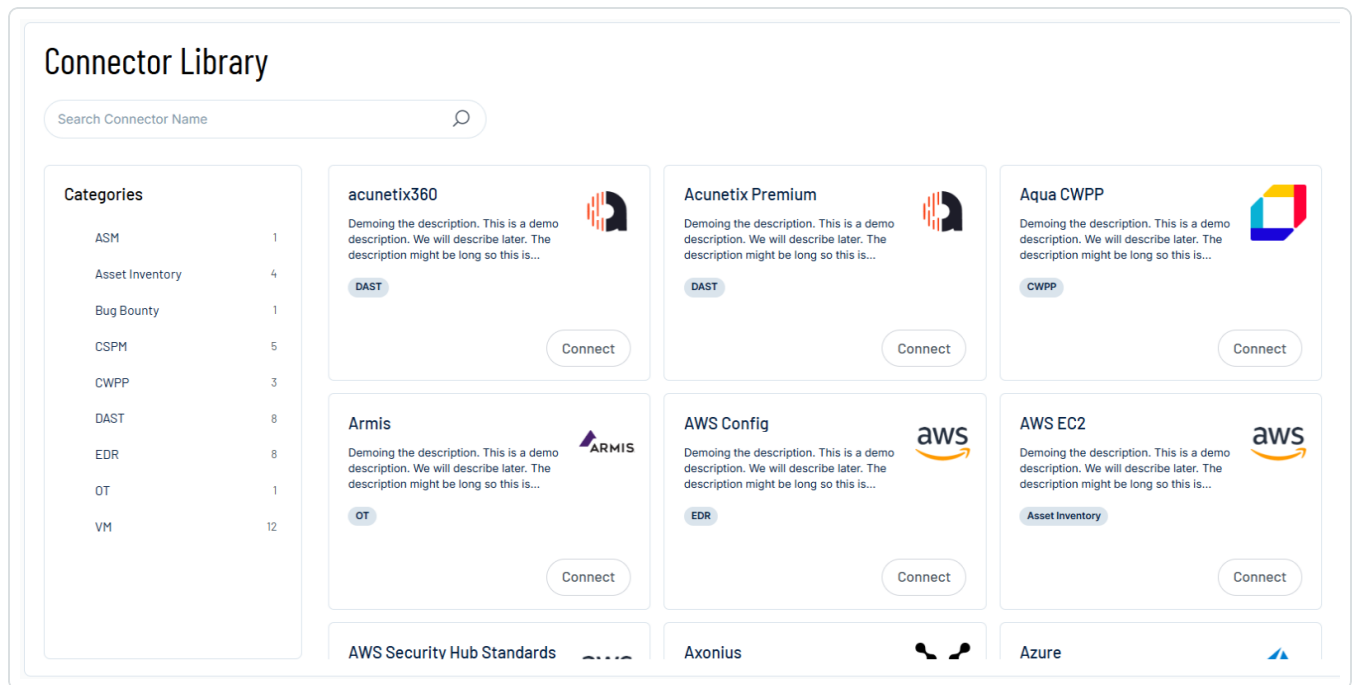
The screenshot shows the "Connectors" page with a search bar, a dropdown menu, and a table of connectors. The table has columns for Name, Connector type, Status, Last data ingestion, and Created on. Each row includes a "Show logs" link and a vertical ellipsis menu icon.

Name	Connector type	Status	Last data ingestion	Created on	
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> ⋮
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> ⋮
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> ⋮

2. In the upper-right corner, click **Add new connector**.



The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. From the **Platform URL** drop-down, select the Cycognito platform URL to use for the connector.
4. In the **API Key** text box, paste the API key you generated earlier.



5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
    - In the **Cycognito asset types to fetch** section, select the check boxes next to the asset types you want to ingest from Cycognito:
      - **Web Applications**
      - **Domains**
      - **IP Addresses**
    - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.
- Tip:** For more information, see [Asset Retention](#).
- For the **Immediately remove assets when their status is** option, choose to automatically remove assets that reach a certain asset status, for example, **Removed**.
6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

⊗ Failed tests 1 out of 4 integration tests failed

Show tests ▾

✓ Successful tests 3 out of 4 integration tests succeeded

Show tests ▾





7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

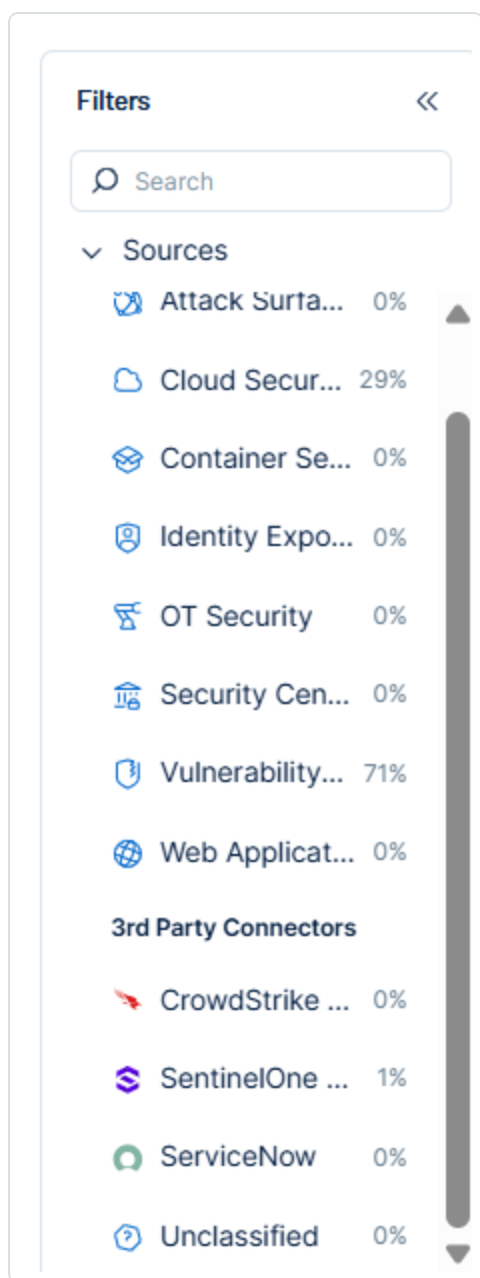
## CyCognito in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

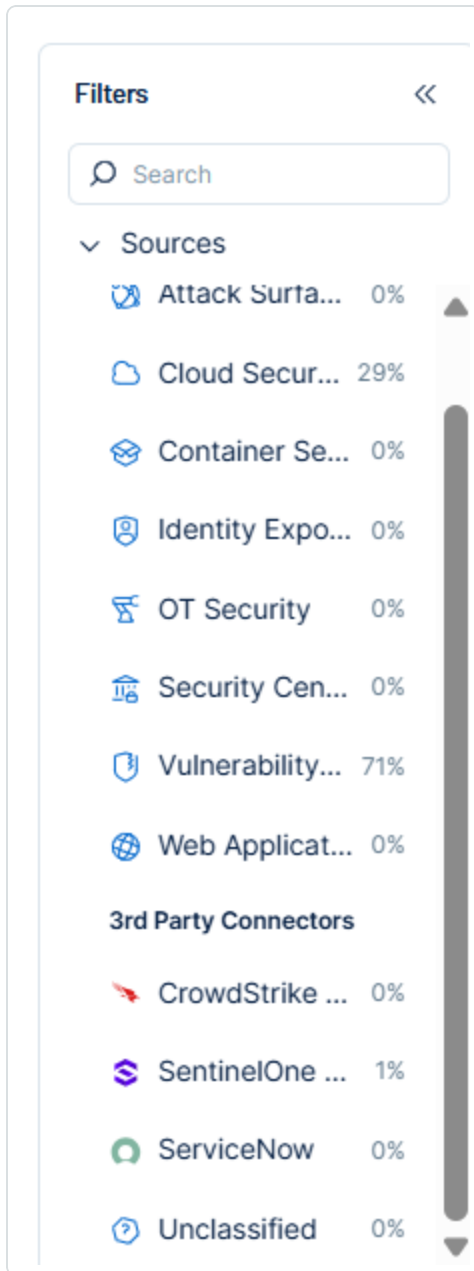
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

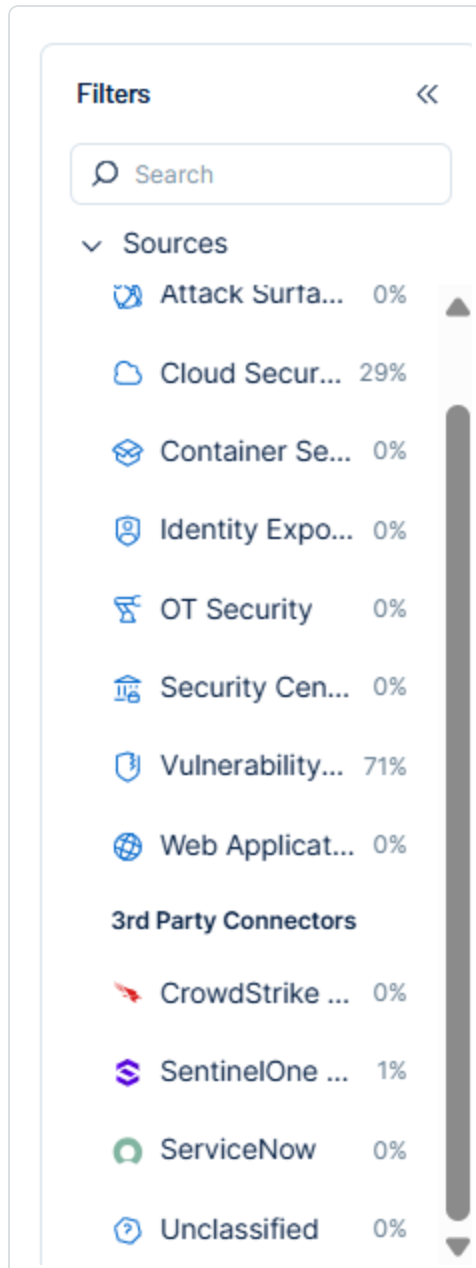
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

### Device Mapping (CyCognito IP Address)

Tenable Exposure Management UI Field	CyCognito Field
Unique Identifier	Asset Id
Asset - Name	IP
Asset - Operating Systems	Platforms
Asset - IPv4 Adresses	IP
Asset - IPv6 Adresses	
Asset - First Observation Date	First Seen
Asset - Last Observed At	Last Seen
Asset - External Tags	Organizations Technical Owner Business Units Asset Type tags
Asset Custom Attributes	type: type score: Security Score grade: Security Grade hosting: Hosting



	<code>discoverability: Discoverability</code> <code>attractiveness: Attractiveness</code> <code>technical_owner: Technical Owner</code> <code>organizations: Organizations</code> <code>locations: Locations</code> <code>environments: Environments</code> <code>ip_ranges: IP Ranges</code>
--	---

### Web Application Mapping (CyCognito Web Applications)

Tenable Exposure Management Value	CyCognito Value
Unique Identifier	Asset Id
Asset - Name	Webapp Address
Asset - First Observation Date	First Seen
Asset - Last Observed At	Last Seen
Asset - Webapp Homepage Screenshot Url	Homepage URL
Asset - External Tags	tags Organizations Technical Owner Business Units Asset Type
Asset Custom Attributes	type score: Security Score grade: Security Grade hosting



	discoverability attractiveness technical_owner organizations
--	---

## Web Application Mapping (CyCognito Domain)

Tenable Exposure Management Value	CyCognito Value
Unique Identifier	Asset Id
Asset - Name	Domain
Asset - First Observation Date	First Seen
Asset - Last Observed At	Last Seen
Asset - Webapp Homepage Screenshot Url	Domain
Asset - External Tags	tags Organizations Technical Owner Business Units Asset Type
Asset Custom Attributes	type score: Security Score grade: Security Grade hosting discoverability attractiveness technical_owner organizations



## Finding Mapping

Tenable Exposure Management UI Field	CyCognito Field
Unique Identifier	Asset Id + id + issue_id
Finding Name	title
CVEs	issue_id
Severity Driver	enhanced_severity_score or severity_score
Description	summary
First Seen	first_detected
Last seen (Observed)	last_detected
Finding Custom Attributes	investigation_status evidence issue_type issue_id status: issue_status severity severity_score base_score: base_severity_score locations confidence exploitation_availability attacker_interest underground_activit detection_complexity





	<code>potential_threat</code> <code>potential_impac</code> <code>references</code>
--	--

## Finding Status Mapping

Tenable Exposure Management Status	CyCognito Status
Active	All other statuses
Fixed	<code>issue-removed</code>

**Note:**For CyCognito, Exposure Management uses the `issue_status` field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	CyCognito Score
Critical	9-10
High	7-8
Medium	4-6
Low	1-3
None	0

**Note:**For CyCognito, Exposure Management uses the `severity_score` field to determine severity. If `severity_score` is not available, Exposure Management uses the `enhanced_severity_score` field from the connector, if provided.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.



Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li><li>Asset that returns from the connector with the state "Removed"</li><li>(Configurable) Asset status changes to one of the selected statuses defined in the <a href="#">Asset Retention</a> configuration: NORMAL, NEW, CHANGED, N/A, or Archived.</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <code>issue_status = issue-removed</code> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	Asset Id
Finding	Asset Id + id + issue_id
Detection	issue_id



## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Asset Ingestion

Asset types are ingested based on user configuration. The supported asset types are:

- Domains
- IP Addresses
- Web Applications

**Certificates** are not supported and are not ingested.

### Asset Archiving

Assets are archived based on their status and user input. Available status values include:

- Normal
- New
- Changed
- Removed
- N/A

By default, only assets marked as **Removed** are archived.

### Findings Ingestion Criteria

- Findings with an **investigation\_status** of archived or resolved are not ingested.
- Findings with an **investigation\_status** of investigated, uninvestigated, or investigating are ingested and considered vulnerable.

### Findings Count Discrepancy



You may observe differences in the number of findings between CyCognito and Exposure Management due to differences in data association logic:

- Exposure Management includes only findings that are directly linked to an asset.
- CyCognito includes findings associated with linked assets.

Example:

If a domain has an IP address mapped to it, and both the domain and the IP each have a distinct finding:

- In Exposure Management, these will appear as two separate assets, each with its own associated finding.
- In CyCognito, both the domain and the IP will be treated as linked assets, and both findings will appear for both assets.

This behavior can result in a higher findings count in CyCognito compared to Tenable.

## API Endpoints in Use

API version: v1

<a href="https://api.platform.cycognito.com/v1/assets/ip">https://api.platform.cycognito.com/v1/assets/ip</a>	Test Connectivity
<a href="https://api.platform.cycognito.com/v1/issues">https://api.platform.cycognito.com/v1/issues</a>	Test Connectivity
<a href="https://api.platform.cycognito.com/v1/export/request/webapp">https://api.platform.cycognito.com/v1/export/request/webapp</a>	Generate asset report
<a href="https://api.platform.cycognito.com/v1/export/request/domain">https://api.platform.cycognito.com/v1/export/request/domain</a>	Generate asset report
<a href="https://api.platform.cycognito.com/v1/export/request/ip">https://api.platform.cycognito.com/v1/export/request/ip</a>	Generate asset report
<a href="https://api.platform.cycognito.com/v1/export/get">https://api.platform.cycognito.com/v1/export/get</a>	Get reports, Assets
<a href="https://api.platform.cycognito.com/v1/issues">https://api.platform.cycognito.com/v1/issues</a>	Findings

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the CyCognito platform.

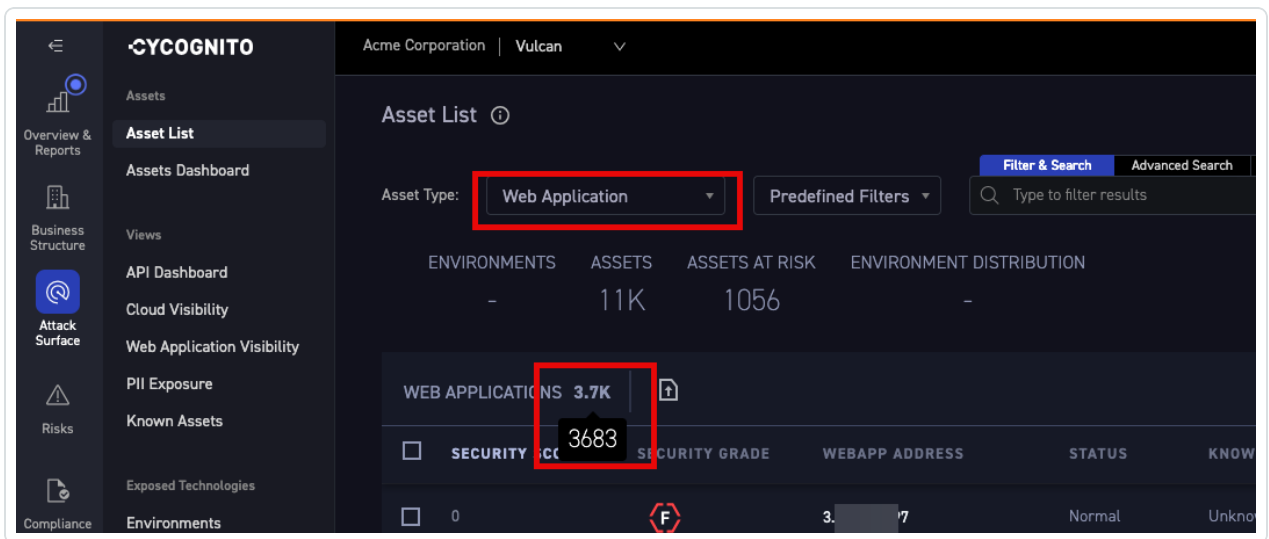


## Asset Data Validation

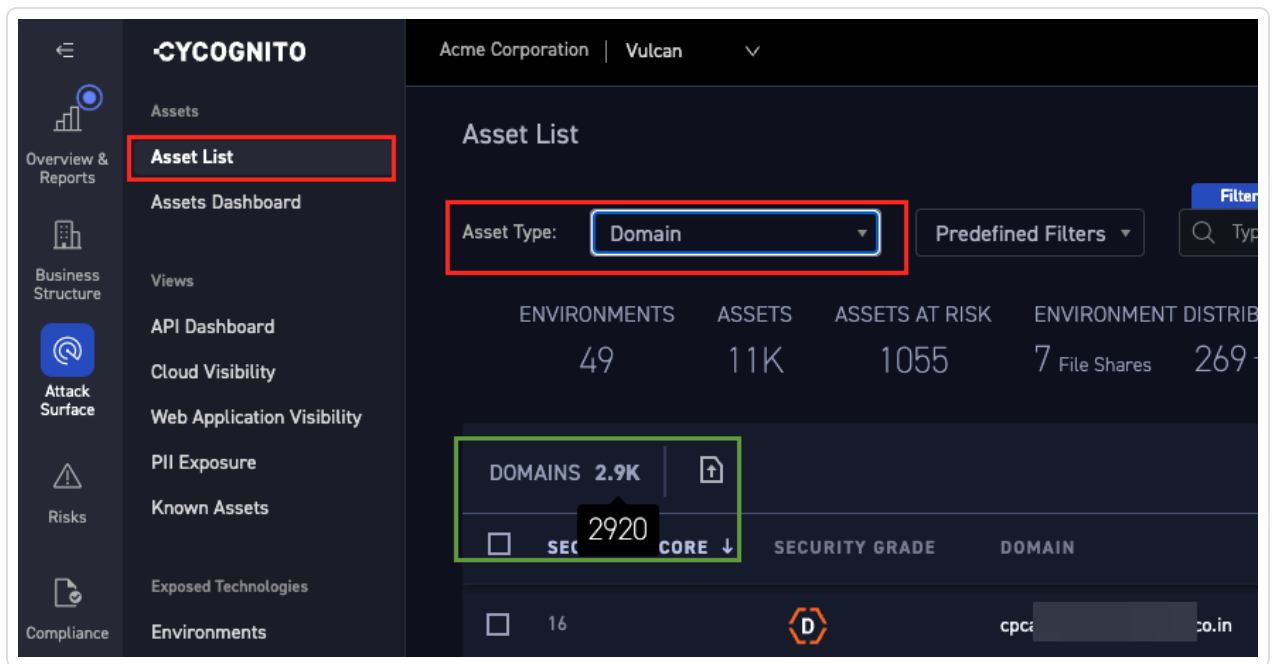
**Objective:** Ensure the number of assets in CyCognito aligns with the number of assets displayed in Tenable Exposure Management.

In CyCognito:

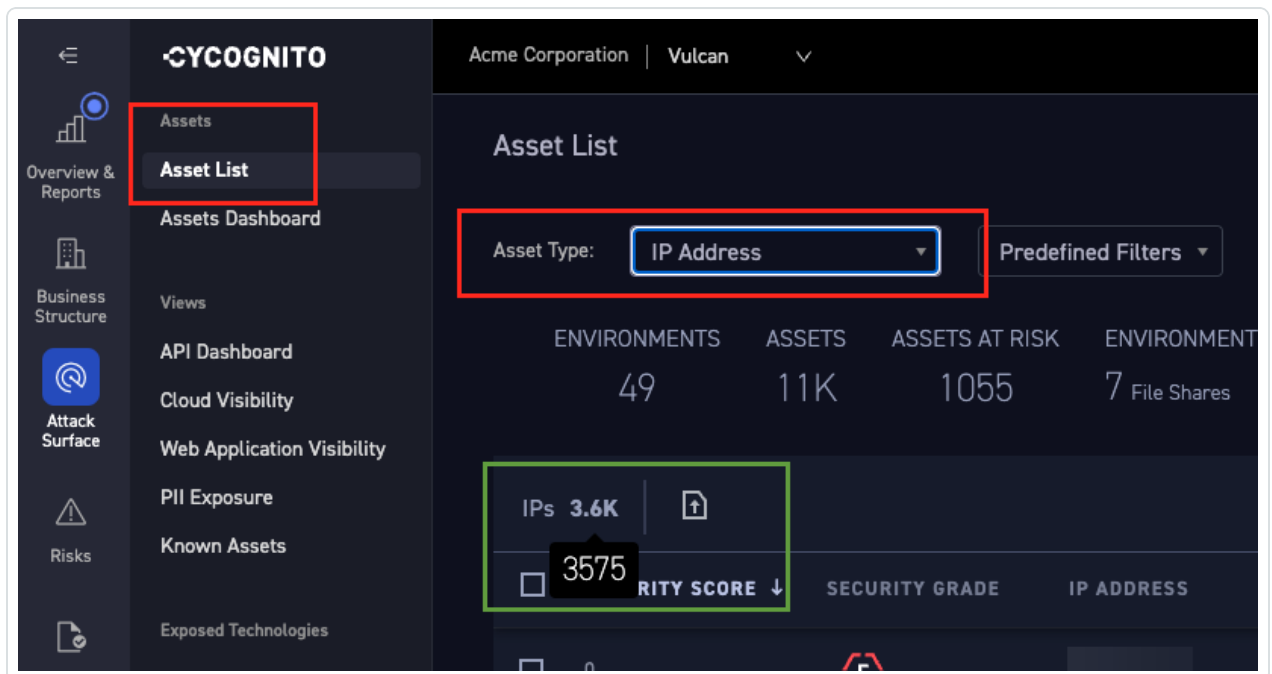
1. Navigate to the **Assets List** > view.
2. Filter by **Asset type** to validate each category:
  - **Web Application:** Select **Web Application** in the **Asset type** filter, then hover over the asset count to view the exact number.



- **Domain:** Select **Domain** in the **Asset type** filter, then hover over the asset count to view the exact number.



- **IP Address:** Select **IP Address** in the **Asset type** filter, then hover over the asset count to view the exact number.



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between CyCognito and Tenable Exposure Management.



**Expected outcome:** The number of assets shown in CyCognito and Exposure Management should match by asset type.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on the last observed date (last seen).
- The asset was archived based its status.
- The asset was archived because it did not return in the connector's next sync.

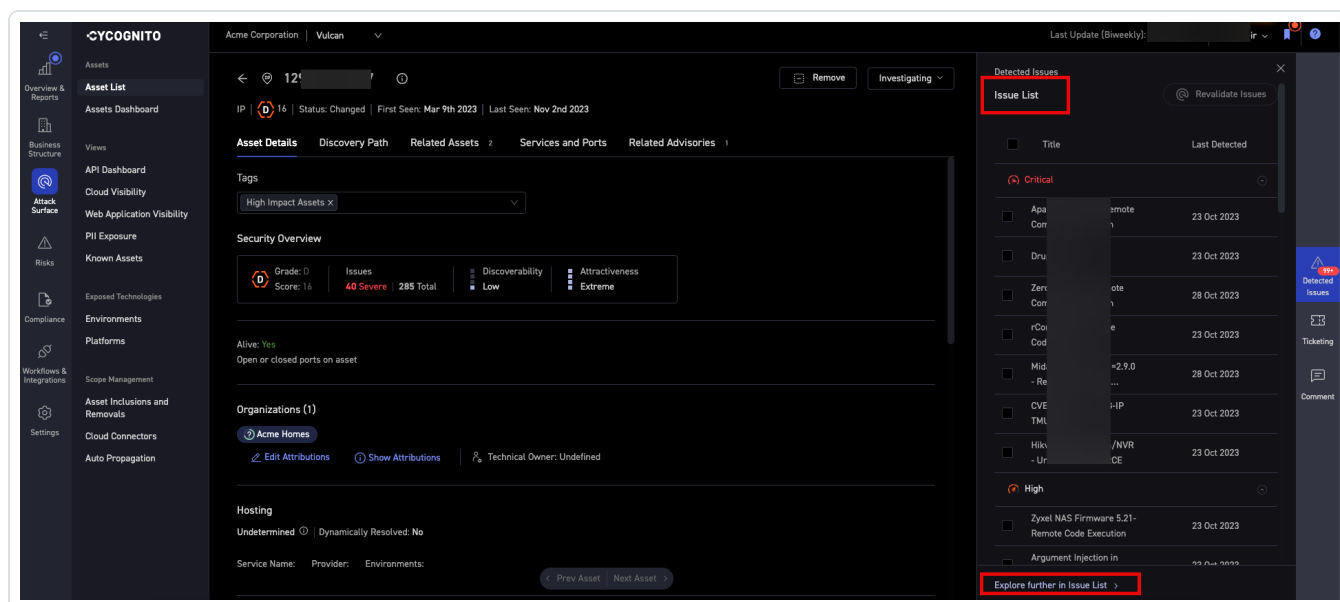
**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the number of findings in CyCognito aligns with the number of findings in Exposure Management.

In CyCognito:

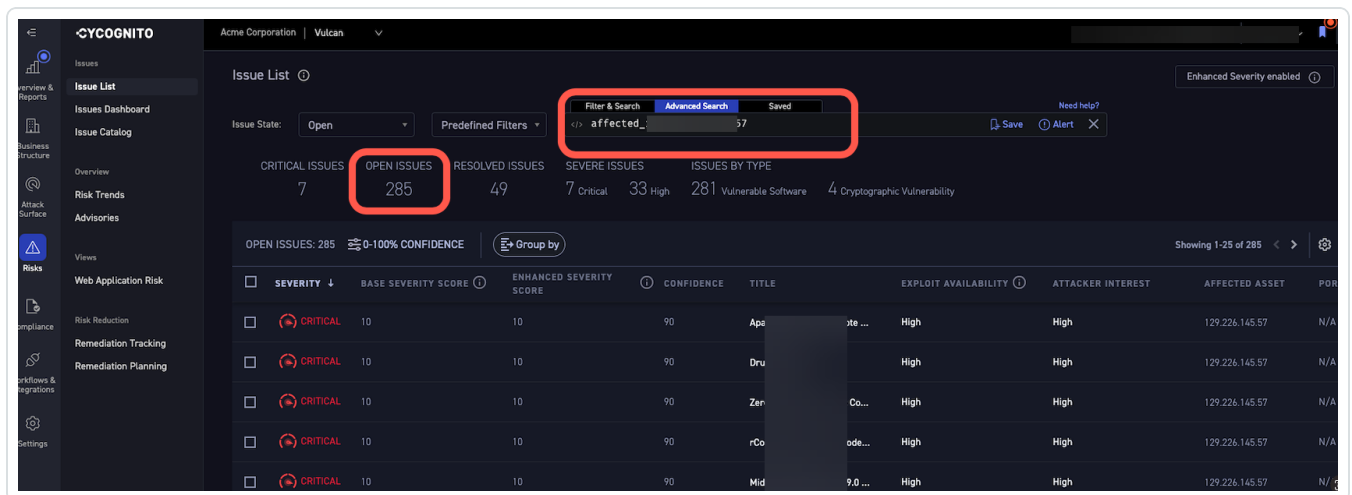
1. Navigate to the **Assets List** and select an asset.
2. In the right panel, review the **Issue List** section.



3. Click **Explore further issues in list** to view the complete issue count for that asset.



You are redirected to the Issues screen, filtered automatically for the selected asset.



In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between CyCognito and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in CyCognito and Exposure Management should match

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## Detectify Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).





[Detectify](#) is a SaaS-based website security service that analyzes and monitors the security level of a user's website by applying a broad range of emulated hacker attacks and providing reports that describe the identified vulnerabilities and their potential risk in the hands of malicious hackers.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Detectify</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Have a [Detectify Enterprise account](#)

- **Generate a Detectify API Key:**

1. Log in to your [Detectify account](#).
2. Click your account name in the upper-left corner of the screen.
3. Select **Account Settings**.
4. Navigate to the **API Keys** tab.


















5. Click **Generate API Key**.
6. If this is your first key, you'll see an empty API key section. If you already have keys, they will appear in a list.
7. Enter a name and optional description for the API key.
8. Click **Generate API Key**.
9. After generation, copy and securely store the API key.
10. Click **Save**.
11. In the **API Key Settings** section, ensure the following permissions are enabled:
  - Allow listing domains
  - Allow reading vulnerabilities
12. Click **Save changes** to apply the settings.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

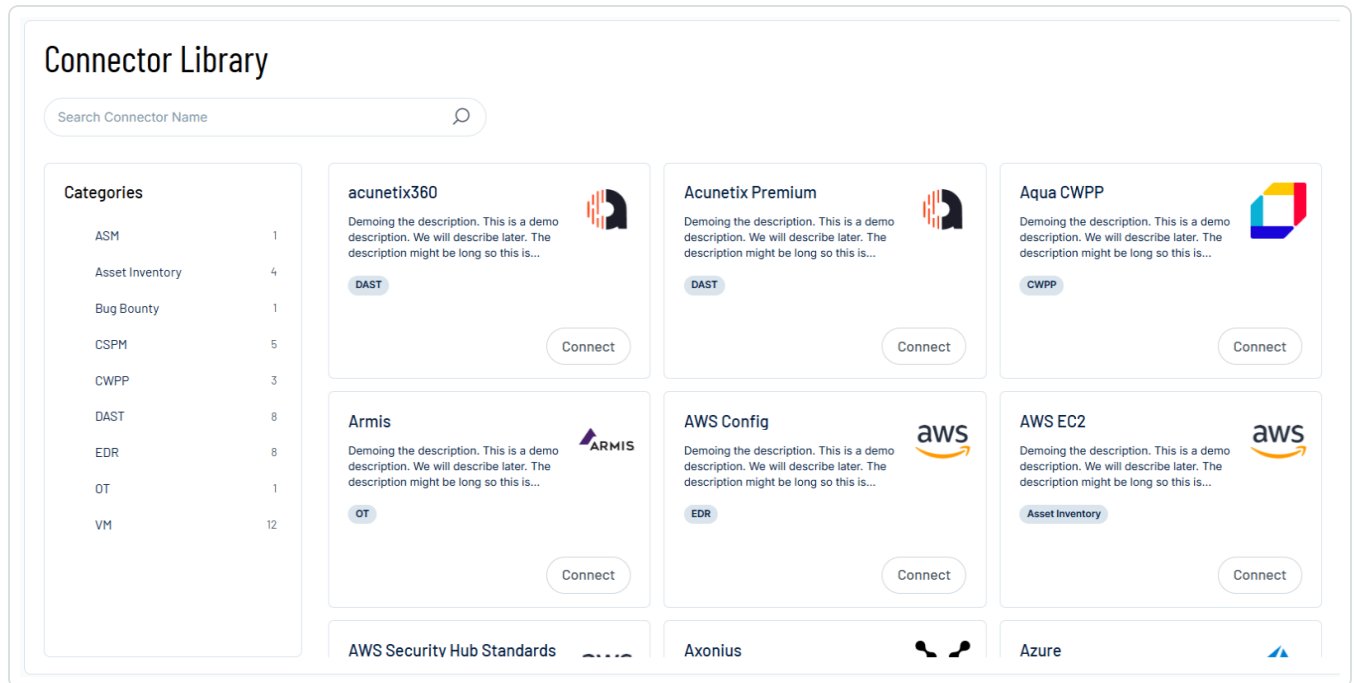
The **Connectors** page appears.

Connectors						
<input type="text" value="Search Connector Name"/>			<input type="text" value="Select"/>			
Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<a href="#">⋮</a>



2. In the upper-right corner, click **+ Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.
4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Key** text box, paste the API key you generated earlier.



4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - Select the relevant fetching options for your integration.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

Show tests ▼

**Successful tests** 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:



- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.

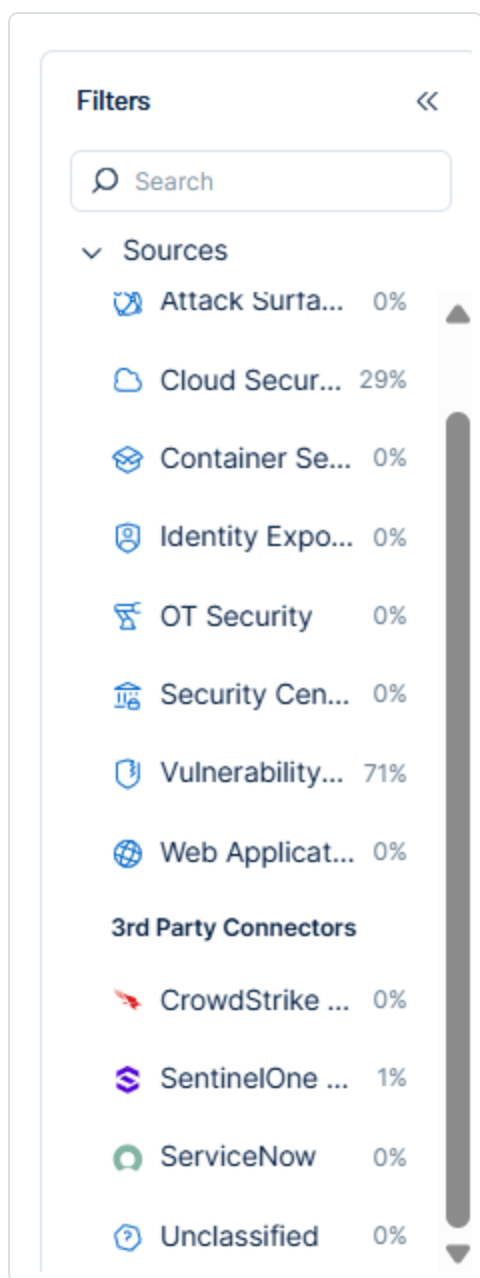
## Detectify in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

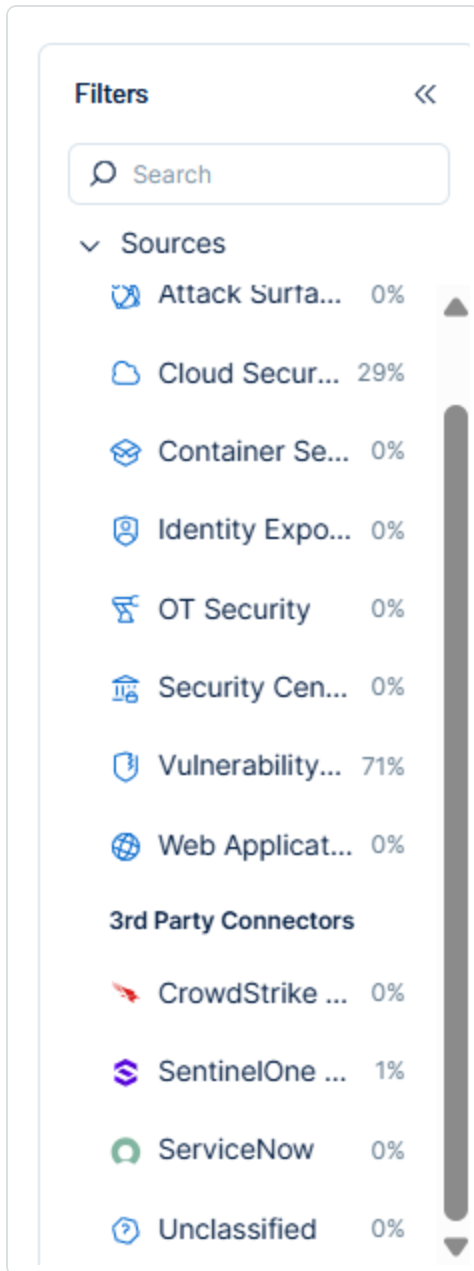
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

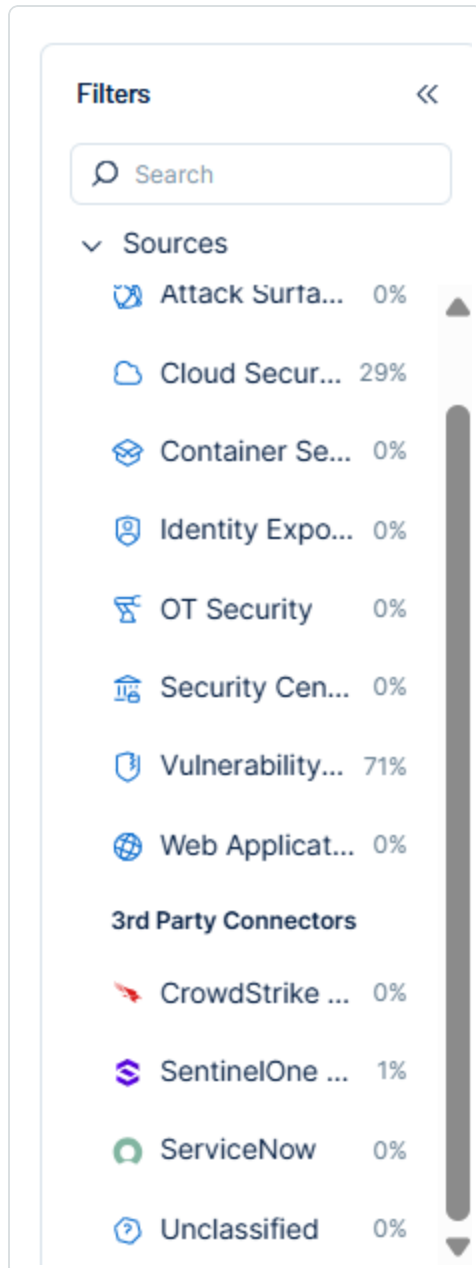
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings







The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management Value	Detectify Value
Unique Identifier	name
Asset - Name	name
Asset - First Observation Date	created
Asset - Last Observed At	last_seen
Asset - Webapp Homepage Screenshot Url	name
Asset - External Tags	domain_type
Asset Custom Attributes	token added_by domain_type

## Finding Mapping

Tenable Exposure Management UI Field	Detectify Field
Unique Identifier	Asset unique id + uuid + Vulnerability unique id
Finding Name	title
CVEs	cwe
Severity Driver	score OR severity



Description	definition.description, definition.risk
First Seen	created_at fallback: timestamp
Last seen (Observed)	updated_at fallback: timestamp
Finding Custom Attributes	location references detectify_tags cvss3_scoring cvss3_severity cvss2_scoring cvss2_severity owasp_year owasp_classification detectify_risk detectify_tags vector detectify_scan_profile_token detectify_asset_vulnerability_connection_ uuid detectify_source detectify_scan_source detectify_details_page

## Finding Status Mapping



Tenable Exposure Management Status	Detectify Status
Active	Active
	New
	Regression
	False Positive
	Accepted Risk
Fixed	Patched

**Note:**For Detectify, Exposure Management uses the `status` field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	Detectify Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:**For Detectify, Exposure Management uses the `score` or `severity` field to determine severity.

## Status Update Mechanisms



Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes Patched on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	name
Finding	Asset unique id + uuid + Vulnerability unique id

## API Endpoints in Use



API version: v2.2.2

		Required Permissions
https://api.detectify.com/rest/v2/assets/	Assets	Allow listing domains
https://api.detectify.com/rest/v2/assets/{domainToken}/subdomains/	Assets	Allow listing domains
https://api.detectify.com/rest/v2/vulnerabilities/	Findings Detection	Allow reading vulnerabilities

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Detectify platform.

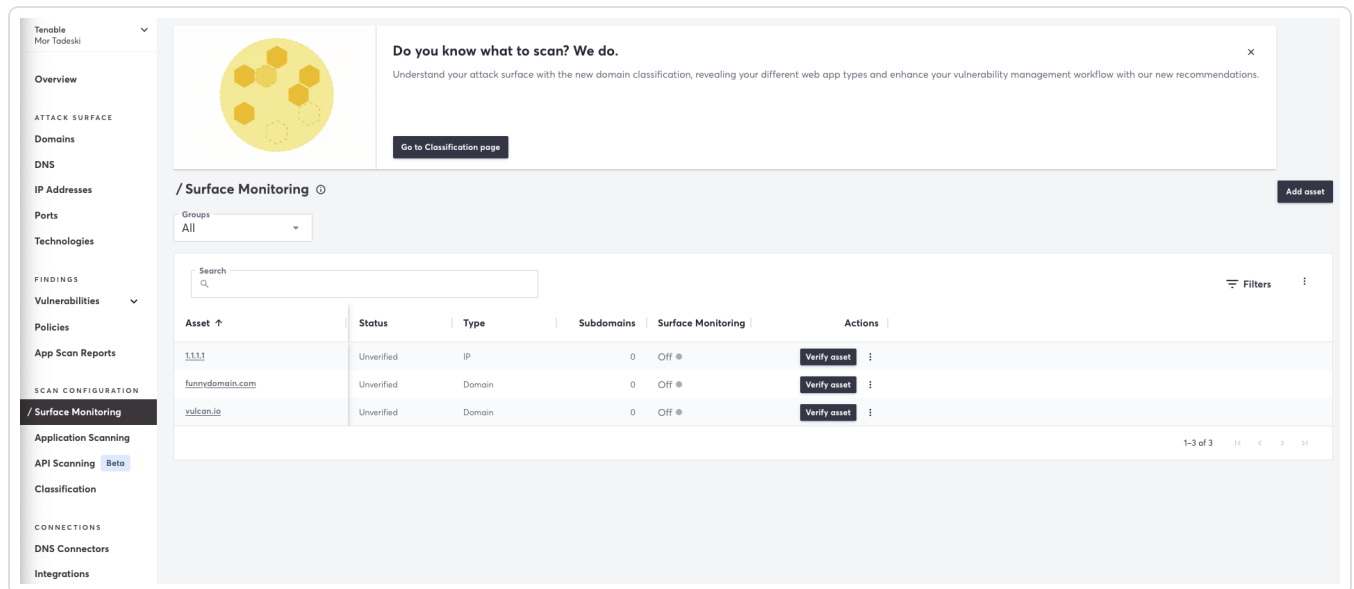
### Asset Data Validation

**Objective:** Ensure the number of scanned domains in Detectify aligns with the web applications displayed in Tenable Exposure Management.

In Detectify:



1. Navigate to the **Surface Monitoring**.
2. The assets list is displayed.



In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between Detectify and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Detectify and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived based on the last observed date (last seen).
- Archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the total number of findings between Detectify and Exposure Management is consistent.

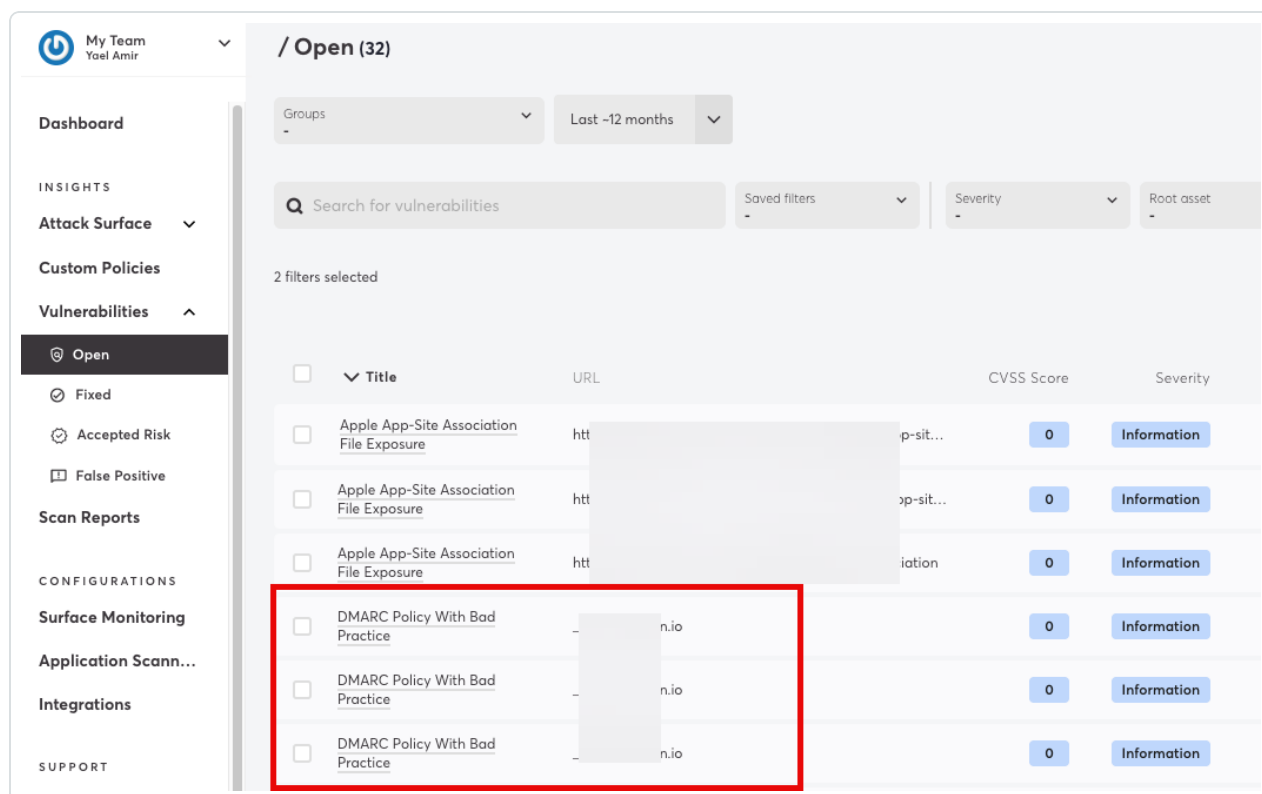
In Detectify:



- In Tenable Exposure Management, ingested vulnerabilities are aggregated and consolidated by uniqueness criteria to deduplicate the data. In Detectify, there is no vulnerability aggregation, and a unique vulnerability with the same URL can be listed several times (based on UUID). Therefore, when validating the data between the Detectify platform and Tenable Exposure Management, it is expected to observe a higher vulnerability count on Detectify than in Tenable Exposure Management.
- Another source for vulnerabilities in Detectify is the **Scan Reports** findings, which is the latest report of each scan profile that reflects the current state of the domain. The data of the report is also ingested into Tenable Exposure Management in addition to the Vulnerabilities Report. However, the findings in the report aren't necessarily exclusive to the report as some of them can also appear in the **Detectify Vulnerabilities Report**.
- The findings of the Scan Reports are aggregated and consolidated into Tenable Exposure Management in the same way as the vulnerabilities findings.
  - Vulnerability instances are identified by their title and the specific URL page.
  - If the same issue is found multiple times on the same URL, each instance is displayed separately in the Detectify UI.
  - Example: The vulnerability DMARC Policy With Bad Practice found three times on the



same URL will appear as three separate entries in Detectify.



In Tenable Exposure Management:

- Exposure Management deduplicates identical issues that occur on the same URL and aggregates them as a single finding.
- In the above example, the three instances of DMARC Policy With Bad Practice on one URL will appear as one finding with that URL as the affected location.

1. [Locate your connector findings.](#)
2. Compare the total number of findings between Detectify and Tenable Exposure Management.

**Expected outcome:** The number of vulnerability instances in Exposure Management will generally be lower than the number displayed in Detectify, due to this aggregation logic.

If a finding is missing from Exposure Management or no longer active, check the following conditions:





- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## HackerOne Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[HackerOne](#) is a vulnerability coordinator and [bug bounty](#) platform that connects businesses with penetration testers and cybersecurity researchers.

The HackerOne platform allows organizations to set their scope, track bug reports, and manage payouts from one location. When integrated with the Tenable Exposure Management, you can review Website vulnerabilities on your assets, while leveraging the power of Tenable Exposure Management discoverability and automation. In this article, you will find how to connect, locate, and automate HackerOne with Tenable Exposure Management.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">HackerOne</a>
Category	Bug Bounty
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable)



	Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Generate HackerOne API Identifier and Token:**

**Note:** Because this is a read-only user, when you create the API identifier, there is no need to assign the identifier or token to a group.

1. In HackerOne, navigate to **Organization Settings > API Tokens**.
2. Click **Create API Token**.
3. Enter an identifier for the new API token. Copy the identifier somewhere safe.
4. Click **Add API token**.
5. Store the generated API token.
6. Click **I have stored the API Token**.

**TIP:** For more information, see HackerOne documentation on [API Tokens](#).

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Identifier** and **API Key** text boxes, paste the API credentials you generated in HackerOne.
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

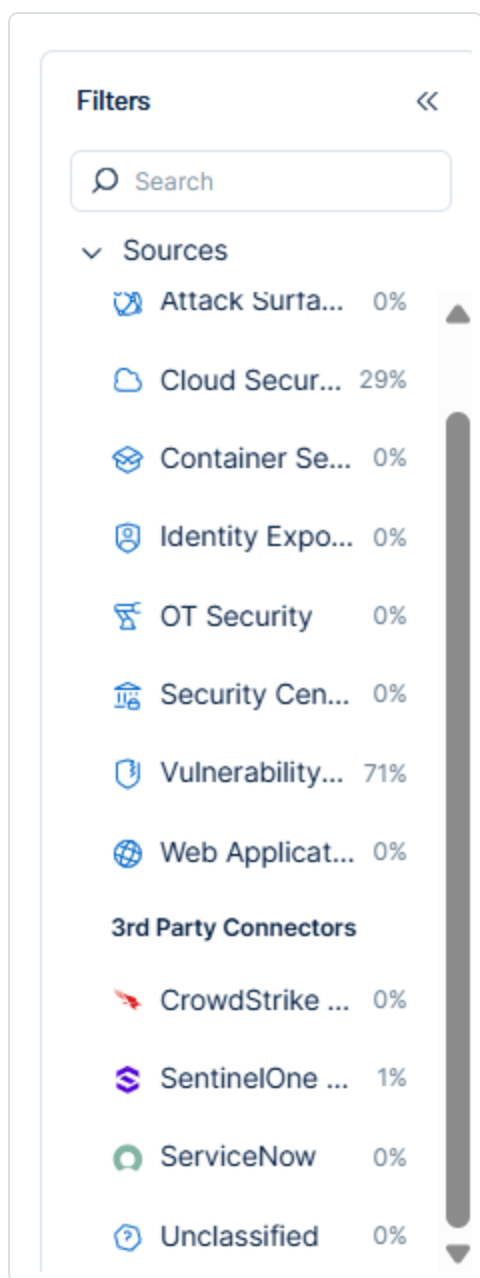
## HackerOne in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

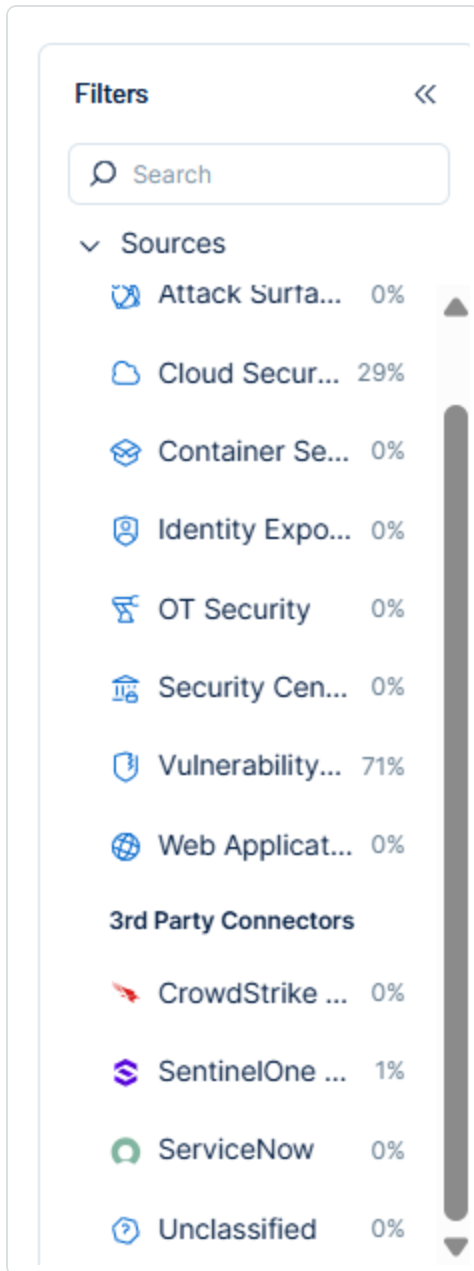
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

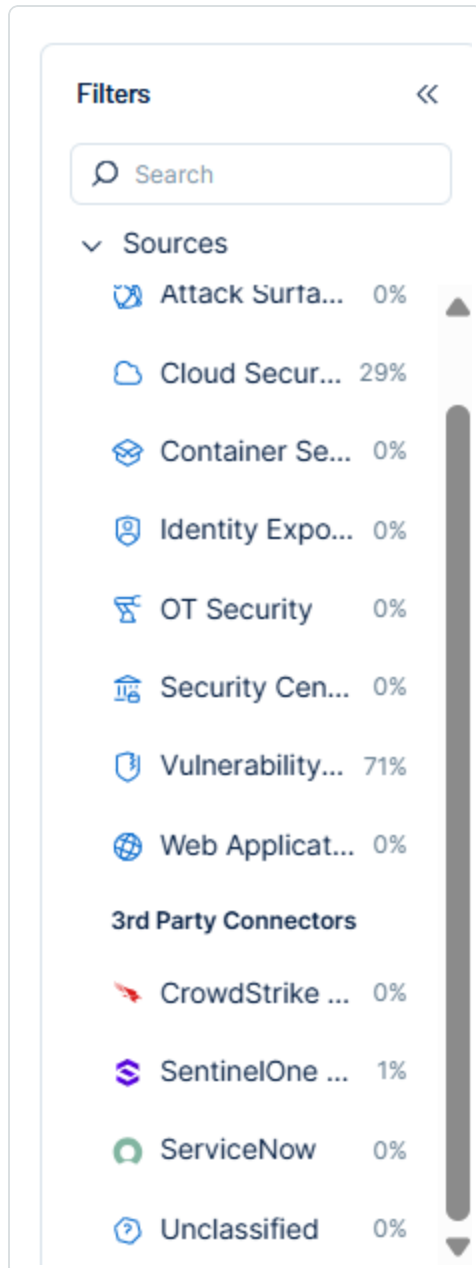
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings







The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management Value	HackerOne Value
Unique Identifier	asset_identifier
Asset - Name	asset_identifier
Asset - First Observation Date	created_at
Asset - Last Observed At	updated_at
Asset - Webapp Homepage Screenshot Url	asset_identifier
Asset - External Tags	handle eligible_for_bounty eligible_for_submission
Asset Custom Attributes	reference max_severity

## Finding Mapping

Tenable Exposure Management UI Field	HackerOne Field
Unique Identifier	asset_identifier + report_id
Finding Name	title



CVEs	cve_ids
CWEs	external_id
Severity Driver	score <b>or</b> rating
Description	vulnerability_information
First Seen	created_at
Last seen (Observed)	last_activity_at
Finding Custom Attributes	custom_fields report_id report_state assigned_to hackerone_rating weakness_type weakness_type_description reporter_name reporter_username attack_vector attack_complexity privileges_required user_interaction scope confidentiality integrity availability



	<code>cvss_score</code> <code>eligible_for_bounty</code> <code>eligible_for_submission</code> <code>relationships.structured_</code> <code>scope.data.attributes.asset_identifier</code>
--	--

## Finding Status Mapping

Tenable Exposure Management Status	HackerOne Status
Active	<code>pre-submission</code> <code>new</code> <code>pending-program-review</code> <code>triaged</code> <code>retesting</code> <code>needs-more-info</code> <code>informative</code> <code>spam</code> <code>duplicate</code> <code>not-applicable</code>
Fixed	Resolved

**Note:**For HackerOne, Exposure Management uses the `state` field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	HackerOneScore
Critical	9-10 <b>Severity: Critical</b>



High	7-8 <b>Severity: High</b>
Medium	4-6 <b>Severity: Medium</b>
Low	1-4 <b>Severity: Low</b>
None	0

**Note:** For HackerOne, Exposure Management uses the `score` field to determine severity. If `score` is not available, Exposure Management uses the `rating` field from the connector, if provided.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>[Finding status changes to <code>finding_status.status = Resolved</code> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria



Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	asset_identifier
Finding	asset_identifier + id
Detection	id

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Asset Mapping

Only website assets are retrieved by the connector.

- In the HackerOne UI, assets are labeled as **Domain**.
- In the API response, the asset type is listed as **URL**.

## API Endpoints in Use

API version: v1

/me/programs	Program ID for following steps
/programs/{programId}	Program handle for following steps and asset enrichment
/programs/{programId}/structured_scopes	Assets (Web applications)



/reports?filter[program[]]=  
{programHandle}

Findings

Detections

## Data Validation

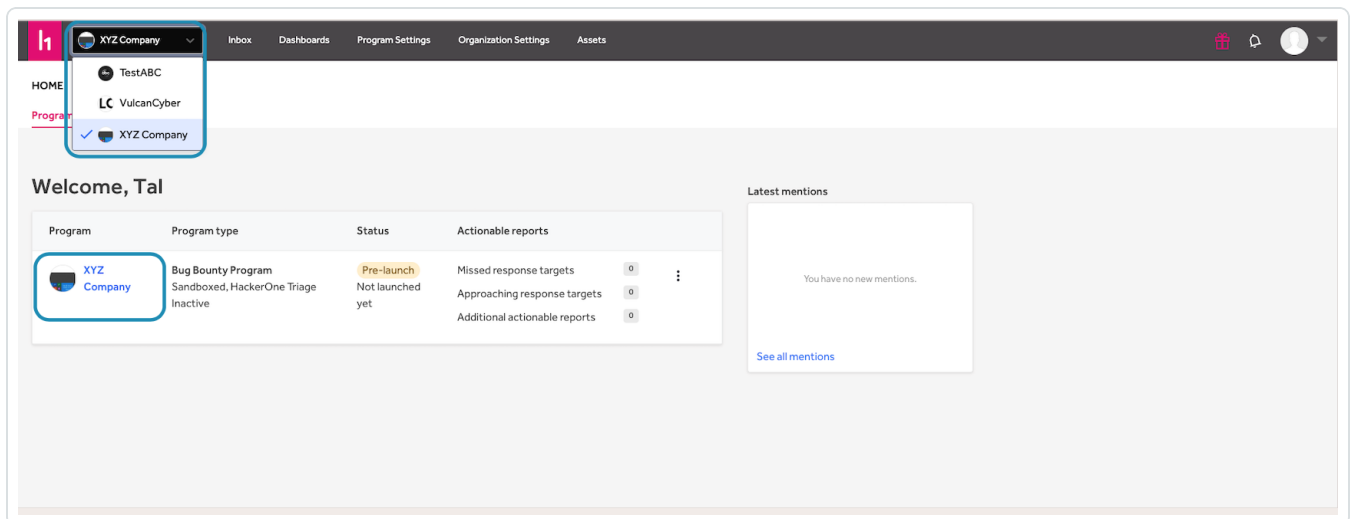
This section shows how to validate and compare data between Tenable Exposure Management and the HackerOne platform.

### Asset Data Validation

**Objective:** Ensure the number of assets (Domains) in HackerOne aligns with the number of assets (Web Applications) displayed in Tenable Exposure Management.

In HackerOne:

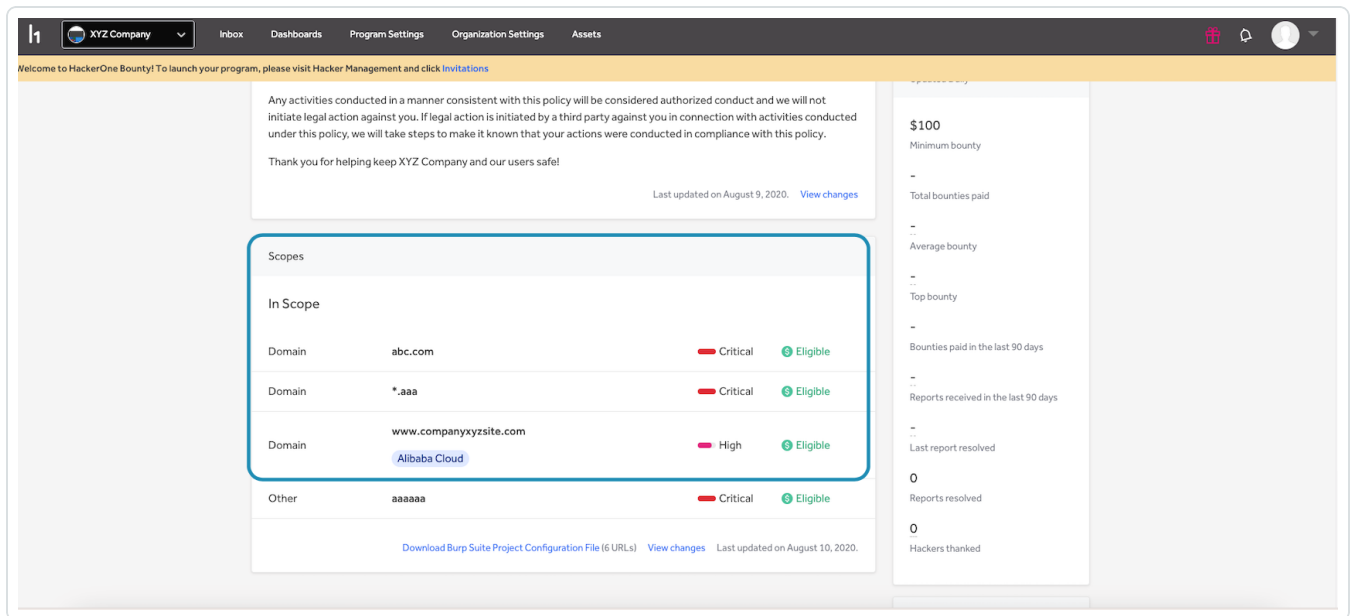
1. From the top menu bar, select the relevant Program/Company name.



2. Scroll down to see the Program assets list in the **Scopes** table.



**Important!** Only **domains** are ingested into the Exposure Management platform.



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between HackerOne and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in HackerOne and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

Finding Data Validation

**Objective:** Ensure that the total number of findings between HackerOne and Exposure Management is consistent.

In HackerOne:



1. Navigate to **Inbox** and note the program reports.

The screenshot shows the Tenable Inbox interface. The top navigation bar includes 'Inbox', 'Dashboards', 'Program Settings', 'Organization Settings', and 'Assets'. A welcome message at the top reads: 'Welcome to HackerOne Bounty! To launch your program, please visit Hacker Management and click Invitations.' Below this, there are tabs for 'New (4)', 'Triaged (2)', 'Assigned to me (0)', 'Pending disclosure (0)', 'Pending bounty (2)', 'Missed Targets (0)', 'All (7)', and 'Custom (6)'. A search bar is present with the text 'Search filtered reports'. A 'Hide filters' button is highlighted with a blue circle. The main content area displays a list of reports on the left and a detailed view of a specific report on the right. The detailed view includes sections for 'Submission dates', 'States' (with checkboxes for Open, Pre-submission, New, Pending program review, Needs more info, Triaged, Retesting, Closed, Duplicate, Informative, N/A, Resolved, Spam), 'Pre-submission' (Accepted, Rejected), and 'Severities' (No Rating, None, Low, Medium). The right sidebar shows details for the selected report, including 'Reported March 31, 2021 5:39pm +0300', 'Participants' (tal\_75a30), 'State' (New (Open)), 'Reported to' (XYZ Company), 'Severity' (High (7.0)), 'Asset: Dom...' (www.companyxyzsite.com), 'Weakness' (Improper Restriction of Authentication Attempts), 'Time spent' (None), 'References' (None), 'Visibility' (Private - Redact), 'CVE ID' (None), 'Assigned to' (None), 'Notificati...' (ON), and 'Account de...' (None).

2. Filter to see only open states (findings).

3. Click on a specific report (finding) to see it's related asset.

The screenshot shows the Tenable Inbox interface with a list of reports on the left and a detailed view of a specific report on the right. The list of reports includes: '#1460780 Test by Roni - 2' (about 1 year ago, Reporter: tal\_75a30, High, Assignee: Team Rocket), '#954306 Demo report: XSS in XYZ Company home page' (about 1 year ago, Reporter: demo-hacker, Low, Assignee: demo-member), '#1143333 Code Injection' (about 1 year ago, Reporter: tal\_75a30, High, Assignee: demo-member), '#1414102 Demo vulnerability 1/12/2021' (about 1 year ago, Reporter: tal\_75a30, Medium), '#1143332 Brute Force Vulnerability' (2 years ago, Reporter: tal\_75a30, High), and '#1058437 Buffer overflow in vendor site' (2 years ago, Reporter: tal\_75a30, High). The detailed view of the selected report '#1460780 Test by Roni - 2' shows a 'Summary' section with a placeholder for a summary of the vulnerability, 'Steps To Reproduce' with a placeholder for details on how to reproduce the issue, 'Supporting Material/References' with a placeholder for additional material, and 'Impact' with the text 'High as the empire test building'. The right sidebar shows details for the selected report, including 'Reported January 26, 2022 5:28pm +0200', 'Participants' (tal\_75a30), 'State' (New (Open)), 'Reported to' (XYZ Company), 'Severity' (High (7.3)), 'Asset: Dom...' (abc.com), 'Weakness' (Allocation of Resources Without Limits or Throttling), 'Time spent' (None), 'References' (None), 'Visibility' (Private - Redact), 'CVE ID' (None), 'Assigned to' (Team Rocket), 'Notificati...' (ON), and 'Account de...' (None).

In Tenable Exposure Management:





1. [Locate your connector findings.](#)
2. Compare the total number of findings between HackerOne and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in HackerOne and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## Intune Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

Microsoft Intune is a cloud-based unified endpoint management platform that empowers IT to manage, assess, and protect apps and devices.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Microsoft Intune</a>
Category	Asset Inventory, Endpoint Security
Ingested data	Assets
Ingested <a href="#">Asset</a>	Device



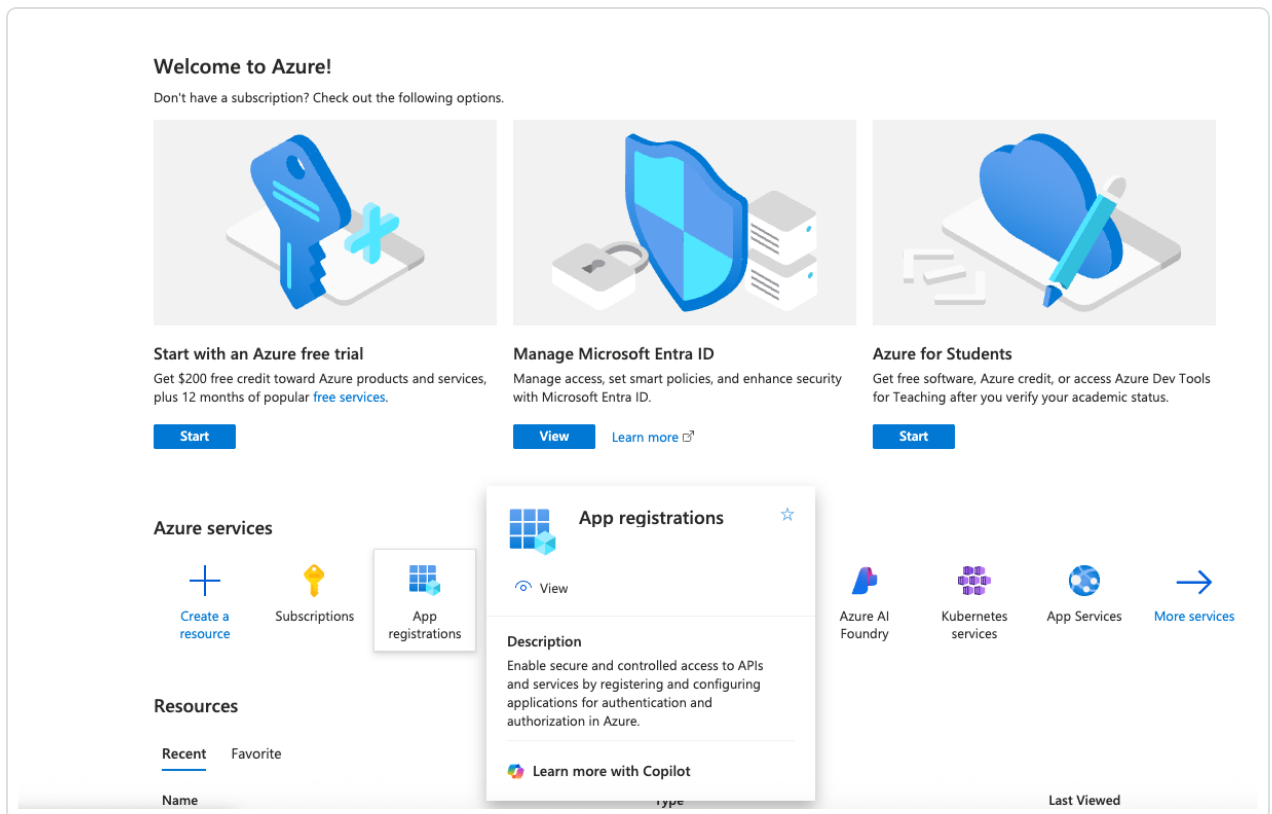
<a href="#">Classes</a>	
Integration type	UNI directional (data is transferred from the connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Register a new application in Azure ID:**

1. In the Microsoft Azure portal, navigate to **App registrations**.



2. Click **New Registration**.

The **Register an application** page appears.



[Home](#) > [App registrations](#) >

## Register an application

**\* Name**

The user-facing display name for this application (this can be changed later).

**Supported account types**

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Vulcan Labs only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

**Redirect URI (optional)**

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼

e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

---

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

### 3. Configure the following application settings:

- **Name** — Type a descriptive name for your application (e.g., "Intune-Integration").
- **Supported account types** — Choose Accounts in this organizational directory only.

### 4. Click **Register** to create the application.

## Get the Azure Application (Client) ID and Directory (Tenant) ID:

1. Navigate to the **Application Overview** page for the application you [created and registered](#) in Microsoft Azure.
2. Copy and save the **Application (Client) ID** and **Directory (Tenant) ID** values for use within Tenable Exposure Management.

## Generate an Azure Client Secret:



1. In the Microsoft Azure portal, navigate to **Certificates & Secrets**.
2. In the **Client secrets** section, click **New Client Secret**.
3. In the **Description** text box, type a brief description of the client secret.
4. In the **Expires** section, select the period after which you want the secret to expire.
5. Click **Add**.
6. Copy and save the client secret value for use within Tenable Exposure Management.

### Assign API Permissions:

To access Intune device data, your application requires specific permissions.

1. In the Microsoft Azure portal, navigate to **API Permissions**.
2. Click **Add a permission > Microsoft Graph**.

The screenshot shows the 'Request API permissions' window in the Microsoft Azure portal. The 'Microsoft Graph' API is highlighted in a red box. The 'Add a permission' button is also highlighted in a red box. The 'Add a permission' button is located in the 'Configured permissions' section, next to the 'Add a permission' link. The 'Add a permission' link is located in the 'Configured permissions' section, next to the 'Add a permission' link.

API / Permissions name	Type	Description	Admin consent requ.
Microsoft Graph (4)			
DeviceManagementApps.Reading	Application	Read Microsoft Intune apps	Yes
DeviceManagementConfiguration.Read	Application	Read Microsoft Intune device configuration and policies	Yes
DeviceManagementManagedDevices.Read	Application	Read Microsoft Intune devices	Yes
User.Read	Delegated	Sign in and read user profile	No

The **Request API Permissions** window appears.

3. Click **Application permissions**.
4. Configure the following group permissions:



- DeviceManagementManagedDevices.Read.All
- DeviceManagementConfiguration.Read.All
- DeviceManagementApps.Read.All

5. Click **Grant admin consent for [Your Organization]**.

A confirmation window appears.

6. Click **Confirm**.

**Note:** If you do not have admin privileges, your administrator must grant consent.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

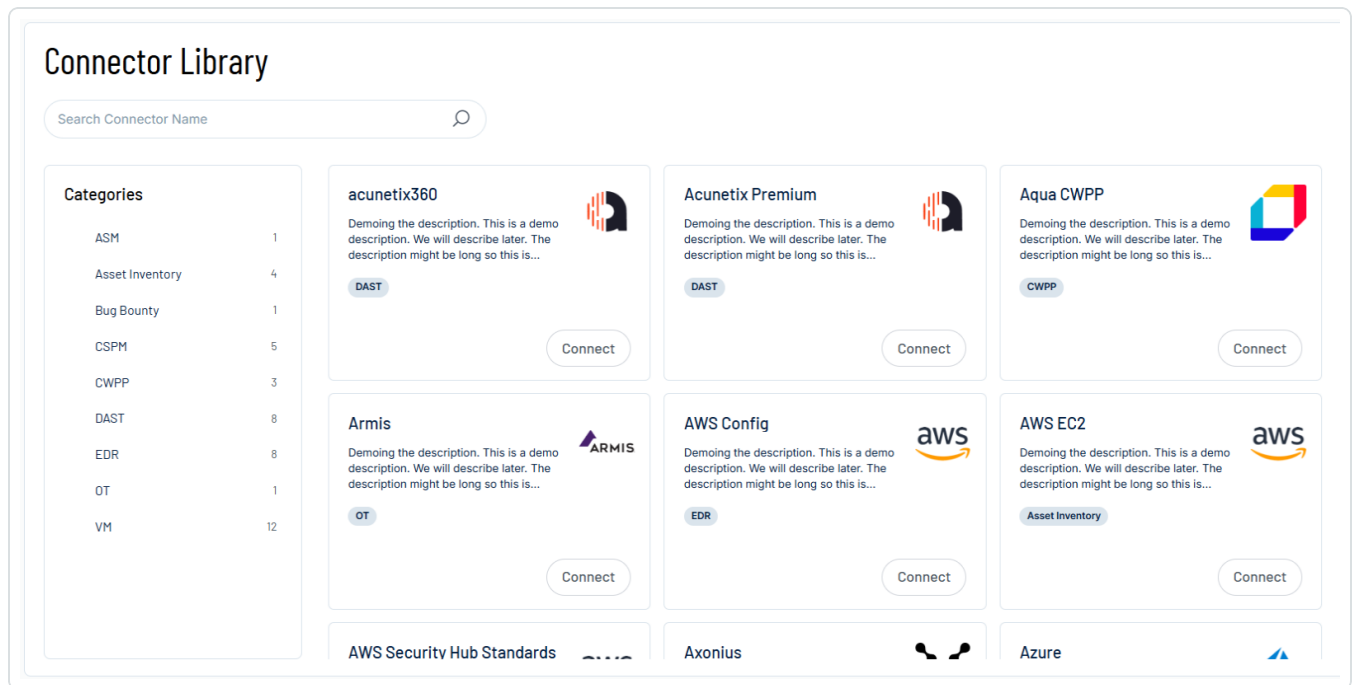
Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

5. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
6. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

7. Enter the credentials you generated earlier (FQDN, API Key, and API ID).
8. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.



- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

9. Click the **Test Connectivity** button to verify that VTenable Exposure Management can connect to your connector instance.

- In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ **Failed tests** 1 out of 4 integration tests failed

Show tests ▼

✔ **Successful tests** 3 out of 4 integration tests succeeded

Show tests ▼

10. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

11. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.

12. To confirm the sync is complete, do the following:



- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.

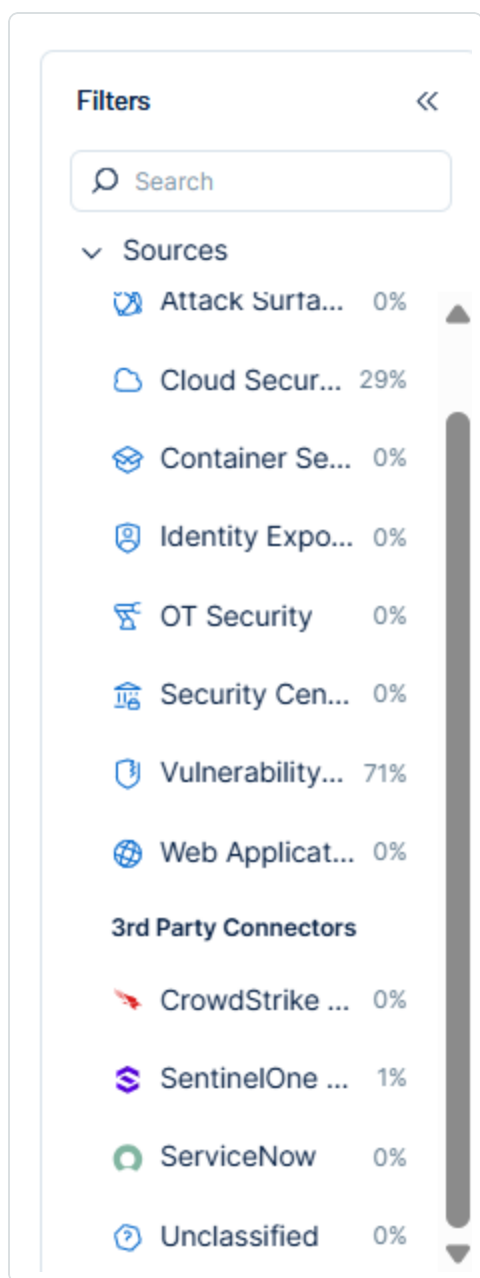
## Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.





The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



Tenable Exposure Management UI Field	Intune Field
Unique Identifier	id
Asset - External Identifier or Asset - Provider Identifier	azureADDeviceId
Asset - Name	deviceName
Asset - Operating Systems	operatingSystem
Asset - MAC Addresses	ethernetMacAddress or wiFiMacAddress
Asset - First Observation Date	enrolledDateTime
Asset - Last Observed At	lastSyncDateTime
Asset - External Tags	<ul style="list-style-type: none"><li>• deviceCategoryDisplayName</li><li>• complianceState</li><li>• deviceRegistrationState</li><li>• managedDeviceOwnerType</li></ul>
Asset Custom Attributes	osVersion

### Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>• Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>• Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>



**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	asset - id

## API Endpoints in Use

Base URL: <https://management.azure.com>

API	Use in Tenable Exposure Management	Requested Permissions
POST - <a href="https://login.microsoftonline.com/{{tenant_id}}/oauth2/v2.0/token">https://login.microsoftonline.com/{{tenant_id}}/oauth2/v2.0/token</a>	Authentication	Read
GET - <a href="https://graph.microsoft.com/v1.0/deviceManagement/managedDevices">https://graph.microsoft.com/v1.0/deviceManagement/managedDevices</a>	Managed Devices - Devices	Read

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.



## Avoiding Sync Loops (Tenable Adapter in Microsoft Intune)

Microsoft Intune may include assets sourced from Tenable via its own Tenable adapter. To prevent sync loops—where assets originating from Tenable are re-ingested back into Tenable — the connector filters out any device whose only associated adapters are Tenable-related.

### Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Microsoft Intune.

#### Asset Data Validation

For each unique asset - id in Microsoft Intune, the Intune connector creates an asset in Exposure Management.

**Objective:** Ensure the number of assets (devices) in Microsoft Intune aligns with the number of devices displayed in Tenable Exposure Management.

In the Microsoft Azure portal:

1. Navigate to the **All Devices** tab.
2. Apply filters to exclude archived devices (based on your configuration in [Asset Retention](#)).

In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between Microsoft Intune and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Microsoft Intune and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

If an asset meets any of the following conditions, it will not appear in Exposure Management.



- Archived based on the last observed date (field last\_seen).
- Asset isn't expected to be fetched because it is already part of [Tenable-Adapters](#).

**Tip:** To learn more on how assets are archived, see [Status Update Mechanisms](#).

## Jamf Pro Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Jamf](#) is a mobile device management system focused on Apple devices. Its main capabilities include Apple devices inventory management, Zero-touch deployments, and controls to manage Apple device security, including enforcement of password policies, enabling remote security features, and fully controlling data stored on a device.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Jamf Pro</a>
Category	Asset Inventory
Ingested data	Assets only
Ingested <a href="#">Asset Classes</a>	Devices
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions



Before you begin configuring the connector, make sure to:

- Identify your Jamf Pro server URL (e.g. `https://yourcompany.jamfcloud.com`).
- Create a Jamf Pro user account (username and password) with **READ** permissions to the Computers API endpoint.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Add new connector

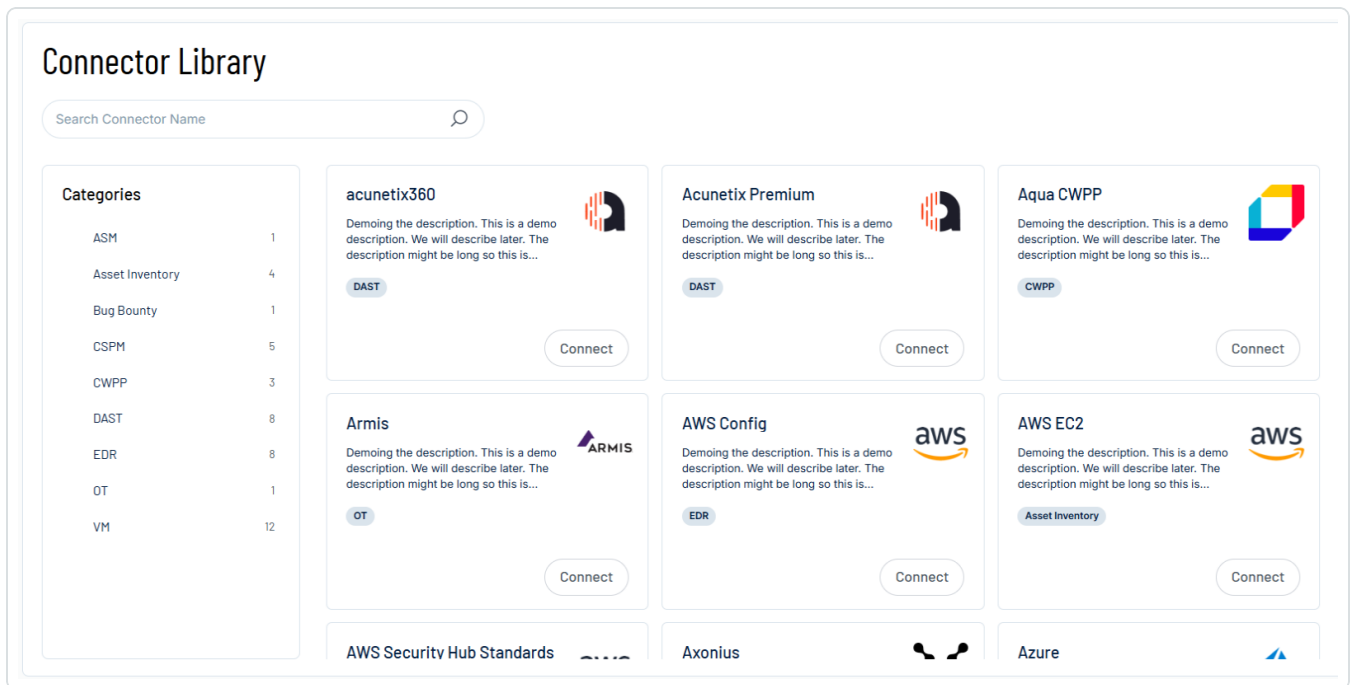
Search Connector Name

Select

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server URL** text box, type the URL of your Jamf Pro server.

4. In the **Username** and **Password** text boxes, paste the credentials for your Jamf Pro account.



5. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.
- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:





- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.

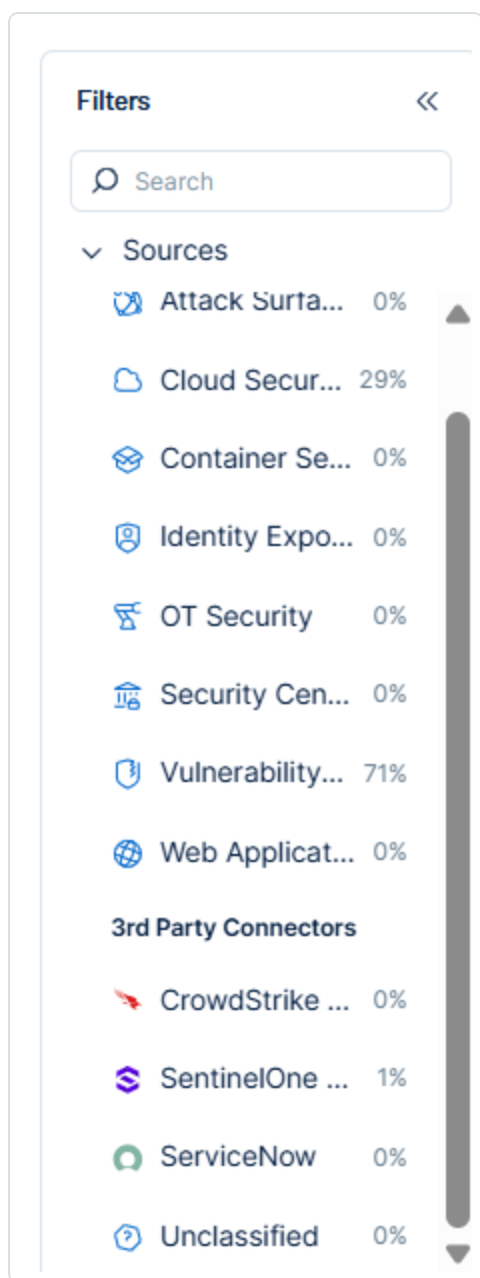
## Jamf Pro in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



Tenable Exposure Management UI Field	Jamf Pro Field
Unique Identifier	id
Asset - Name	general.name or udid
Asset - Operating Systems	operatingSystem.name
Asset - IPv4 Adresses	general.lastReportedIp
Asset - IPv6 Adresses	
Asset - MAC Addresses	hardware.macAddress
Asset - First Observation Date	initialEntryDate
Asset - External Tags	assetTag
	site.name
Asset Custom Attributes	operatingSystem.version
	general.platform
	udid
	hardware.serialNumber
	general.barcode1
	general.barcode2
	general.site.name
	general.remoteManagement.managed
	userAndLocation.username
	userAndLocation.realname
	userAndLocation.email
	userAndLocation.phone
	hardware.make
	hardware.model



hardware.modelIdentifier

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id

## API Endpoints in Use

API version: starting from v10.25.0

		Required Permissions
api/v1/auth/token		Read



api/v1/computers-inventory

Computer Inventory - Device Assets

Read

## Data Validation

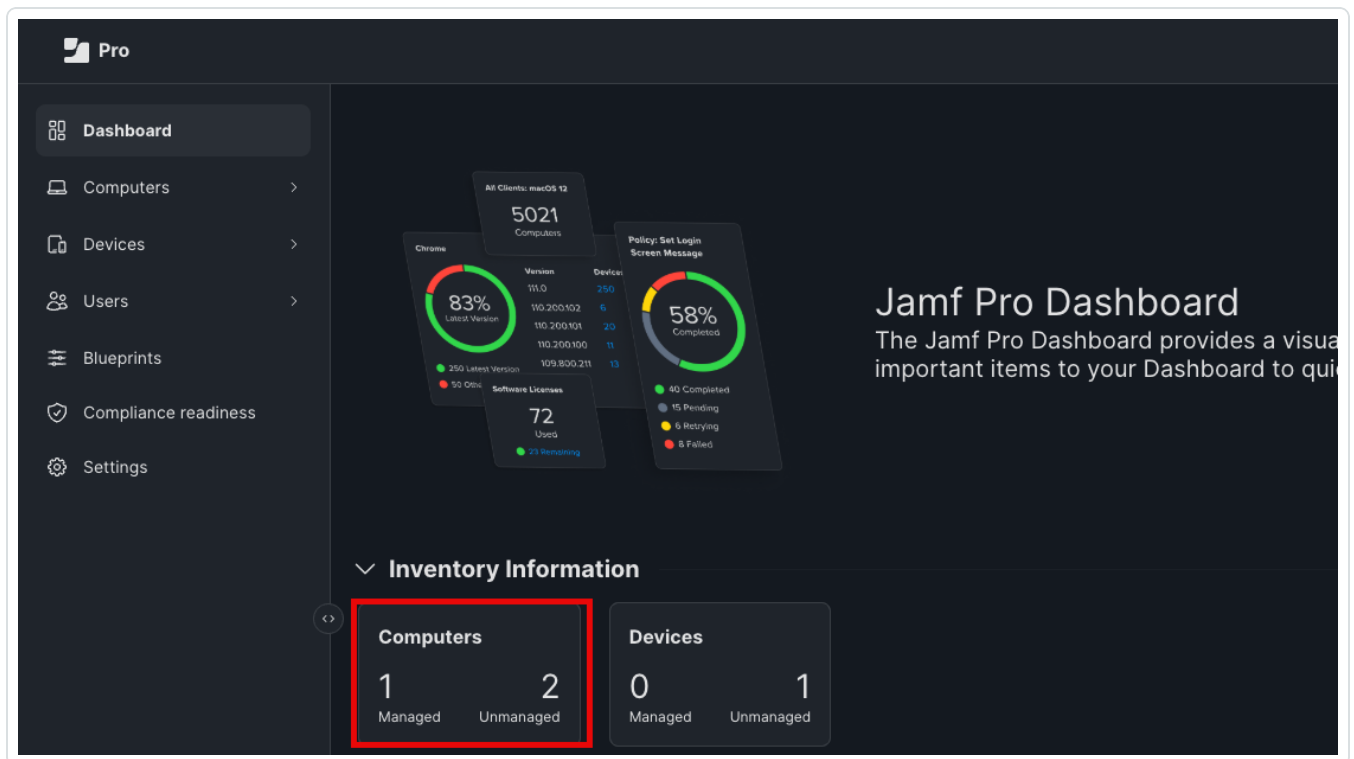
This section shows how to validate and compare data between Tenable Exposure Management and the Jamf Pro platform.

### Asset Data Validation

**Objective:** Ensure the number of endpoints (devices) in Jamf Pro aligns with the number of devices displayed in Tenable Exposure Management.

In Jamf Pro:

1. Navigate to **Dashboard**.
2. Note the number of **Managed** and **Unmanaged** Computers.



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Jamf Pro and Tenable Exposure Management.



**Expected outcome:** The total numbers returned in Jamf Pro and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived based on the last observed date (last seen).

**Tip:** To learn more on how assets and findings change status, see [Jamf Pro Connector](#).

## Microsoft TVM Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Microsoft TVM](#) delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Microsoft TVM rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Microsoft TVM</a>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)

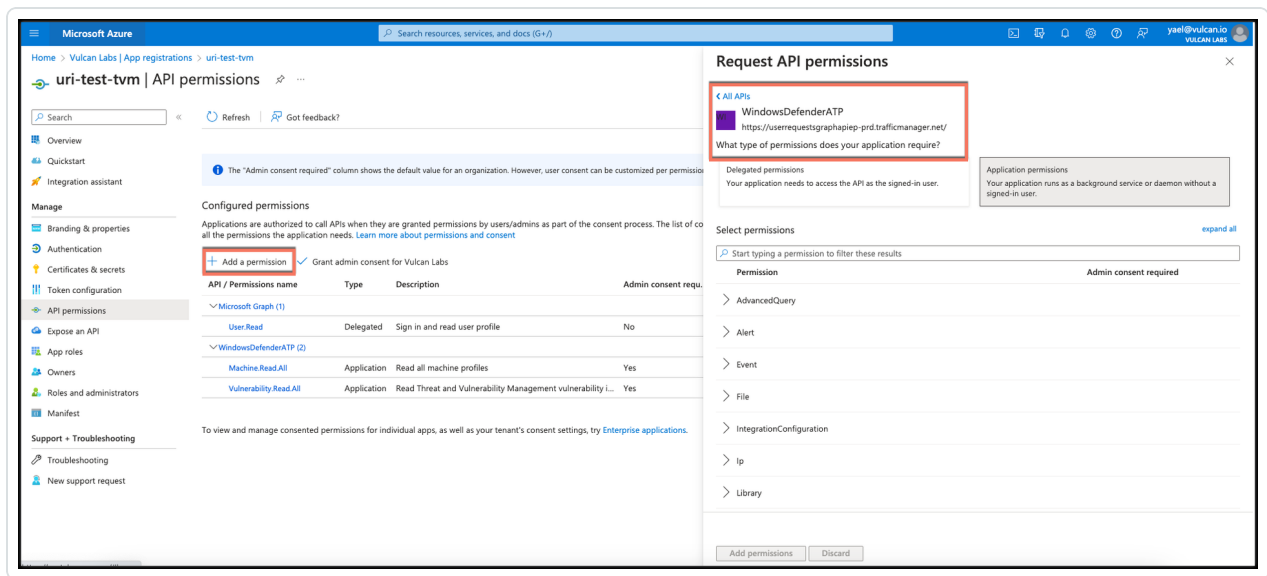


Supported version and type	SaaS (latest)
----------------------------	---------------

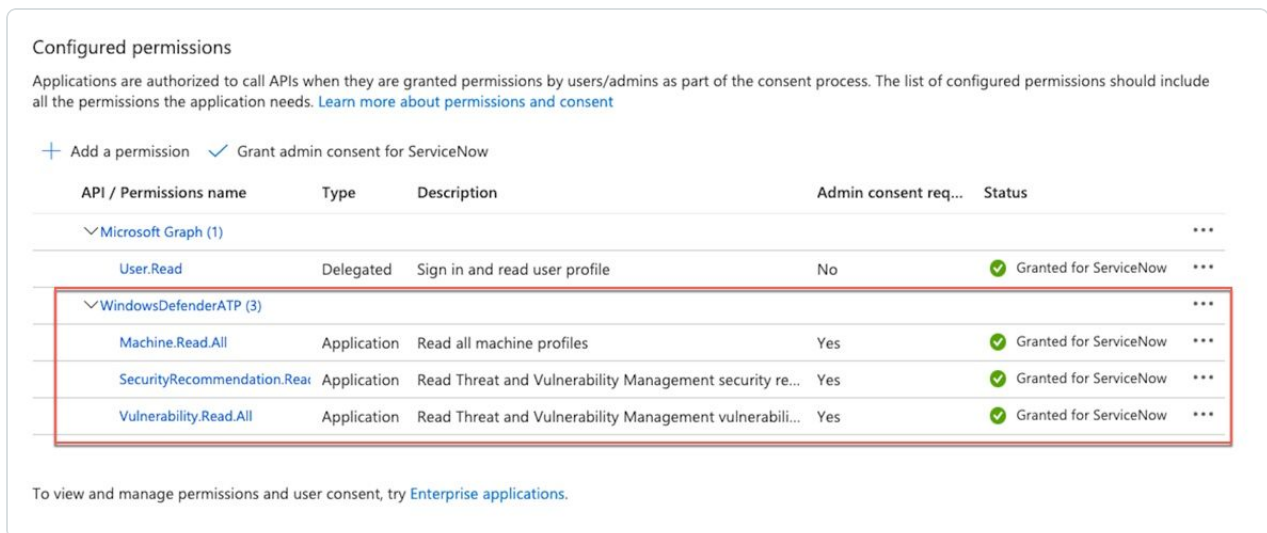
## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Register a Microsoft TVM application, generate Client and Tenant ID, and grant the required access permissions:**
  1. Log in to the Microsoft Azure portal using your Azure portal administrator credentials.
  2. In the left navigation panel on the **Home** pane, click **Azure Active Directory**.
  3. In the **Overview** pane, click **App Registrations**.
  4. In the **App Registrations (Preview)** pane, click **New Registration**. The **Register an application** form appears.
  5. Configure the following options:
    - **Name** - Enter a name for the integration, for example: *Tenable Cyber MS TVM integration*
    - **Supported account types** - Accounts in this organizational directory only
  6. Click **Register**.
  7. The **Application (client) ID** and **Directory (tenant) ID** are now generated. You will need these credentials later when you configure the connector in Tenable Exposure Management.
  8. When the **Application (client) ID** appears in the *Tenable Cyber MS TVM* integration pane, click **Add API permissions**.
  9. Navigate to **APIs my organization uses** and click **WindowsDefenderATP**.



10. In the **API permissions** pane of the *Tenable Cyber MS TVM* integration, click **Add a permission**.
11. Provide **read** access to machines, vulnerabilities, and security recommendations.



12. Click **Grant Admin Consent for <your organization name>**.
13. Navigate to *Tenable Cyber MS TVM* integration > **Certificates & secrets**.
14. Click **New client secret**.
15. In the **Client secrets** form, fill in the required fields:





- **Description** – Enter a name or description for the secret.
- **Expires** – Select the appropriate expiration period.

16. Click **Add**.

The **Value** field populates with your new client secret. This value functions as the password for the integration.

**Important!** You will need this password when configuring the connector in Exposure Management. Save it in a secure location. After you leave this page, the secret will no longer be accessible.

## Add a Connector

To add a new connector:

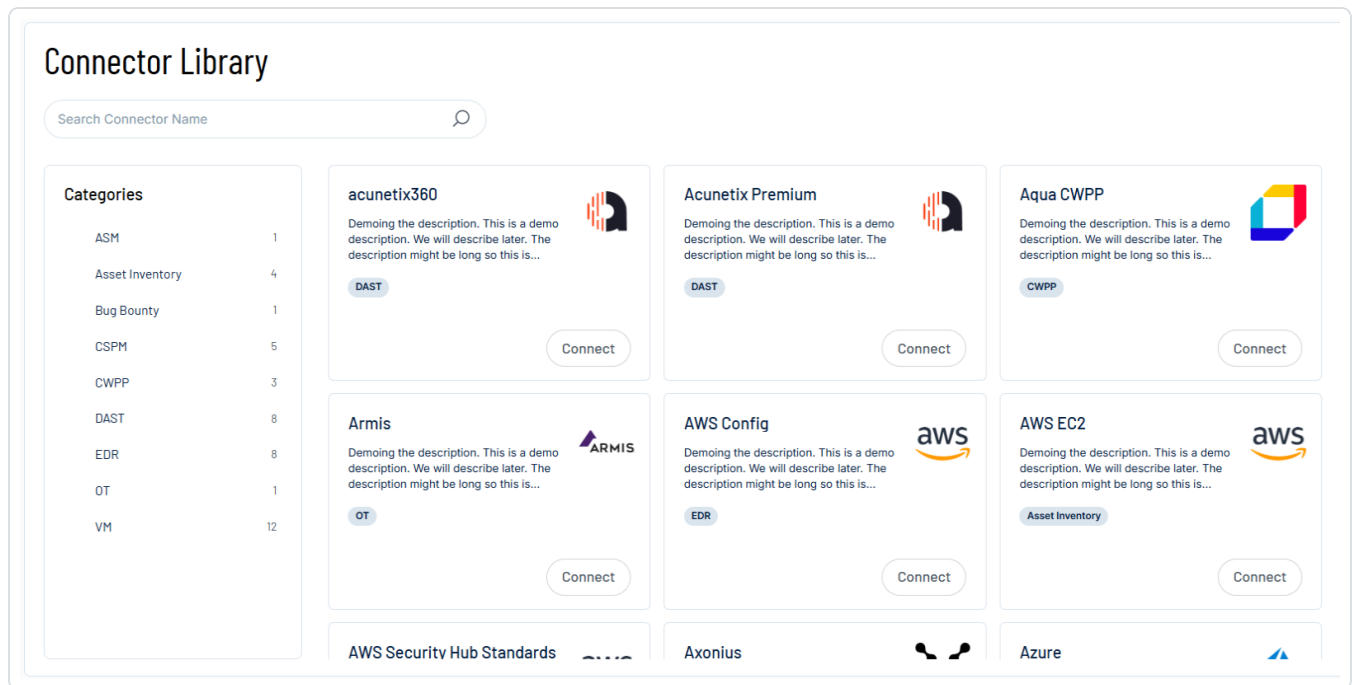
1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Tenant ID**, enter your [Tenant ID](#).
4. In the **App ID** (Application) ID and Client **Secret Value** fields, enter the corresponding credentials you generated in Microsoft Azure.



5. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.
- In the **Set the integration data pulling** section, select the **Map External IP to Asset** and/or **Fetch only onboarded assets** if relevant to your connector needs.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) From the drop-down menu, you can choose to automatically remove assets that reach a certain asset status, for example, **Inactive**.
6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

❌ Failed tests 1 out of 4 integration tests failed

🟢 Successful tests 3 out of 4 integration tests succeeded

[Test connectivity](#)  
[Show tests](#)   
[Show tests](#)

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).



8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

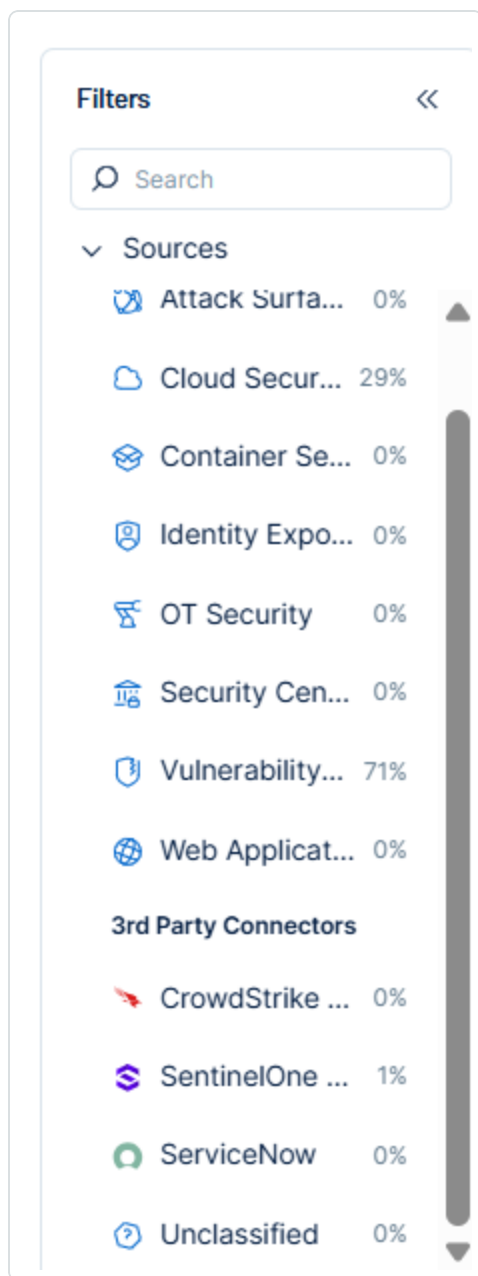
## Microsoft TVM in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

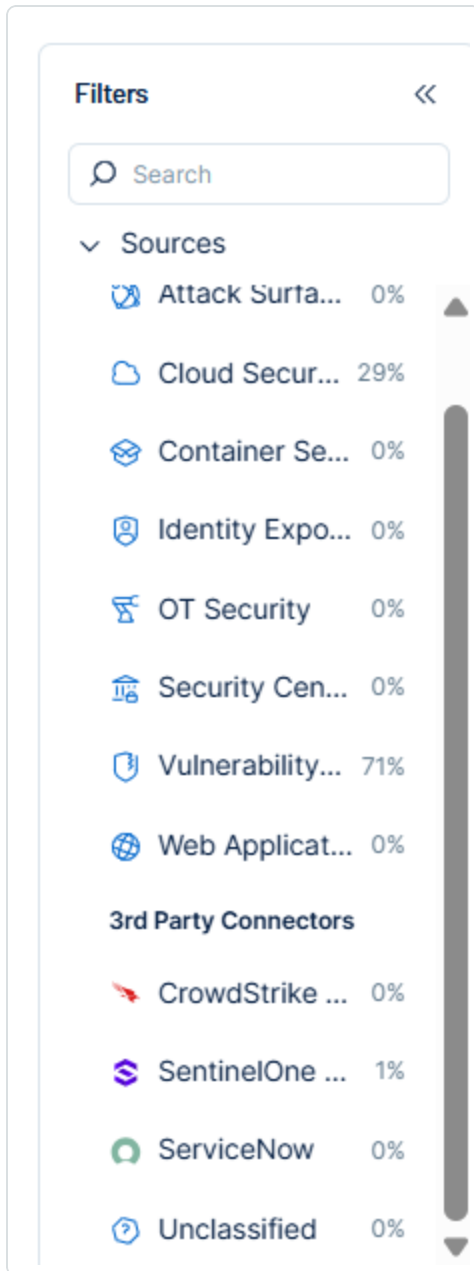
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

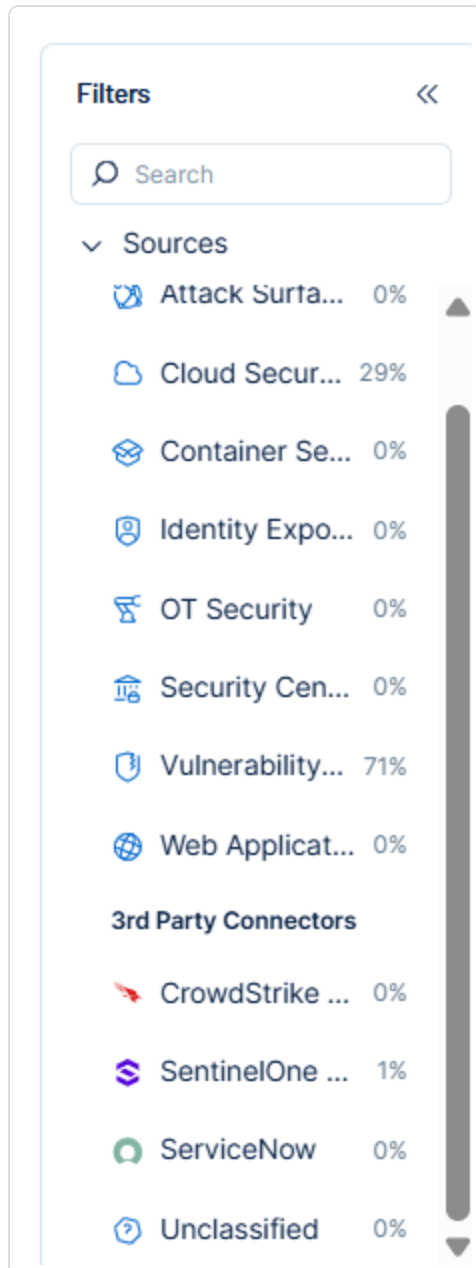
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Microsoft TVM Field
Unique Identifier	id
Asset - External Identifier or Asset - Provider Identifier	vmMetadata.vmId or id
Asset - Name	ComputerDnsName or lastIpAddress or lastExternalIpAddress or id
Asset - Operating Systems	osPlatform
Asset - IPv4 Adresses Asset - IPv6 Adresses	lastIpAddress and lastExternalIpAddress
Asset - First Observation Date	firstSeen
Asset - Last Observed At	lastSeen
Asset - External Tags	machineTags computerDnsName rbacGroupName healthStatus riskScore





	<code>managedBy</code> <code>exposureLevel</code> <code>lastExternalIpAddress</code> <code>osPlatform</code>
Asset Custom Attributes	<code>device_id: id</code> <code>healthStatus: healthStatus</code> <code>exposureLevel: exposureLevel</code> <code>osBuild: osBuild</code> <code>osVersion or version</code>

## Finding Mapping

Tenable Exposure Management UI Field	Microsoft TVM Field
Unique Identifier	<code>cveId + id + deviceId</code>
Finding Name	<code>cveId</code>
CVEs	<code>cveId</code>
Severity Driver	<code>cvssScore</code> or <code>vulnerabilitySeverityLevel</code>
Description	<code>data.description</code>
Finding Custom Attributes	<code>data.cvssVector</code> <code>software_vendor</code> <code>software_name</code> <code>software_version</code> <code>disk_paths</code> <code>registry_paths</code>



	<code>recommended_security_update:</code> <code>recommendedSecurityUpdate +</code> <code>recommendedSecurityUpdateUrl</code>  <code>severity: vulnerabilitySeverityLevel</code>
First Seen	<code>firstSeenTimestamp</code>
Last seen (Observed)	<code>lastSeenTimestamp</code>

### Finding Status Mapping

Tenable Exposure Management Status	Microsoft TVM Status
Active	New or Updated
Fixed	Fixed

**Note:**For Microsoft TVM, Exposure Management ingests only active/vulnerable findings.

### Finding Severity Mapping

Tenable Exposure Management Severity	Microsoft TVM Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty



**Note:** For Microsoft TVM data, Tenable uses the `cvssScore` field to determine severity. If `cvssScore` is not available, Tenable uses the `vulnerabilitySeverityLevel` field from the connector, if provided.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>- Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>- Asset that returns from the connector with the state "healthStatus"</li><li>- Asset not seen for X days according to <b>Last Seen</b>. See <a href="#">Asset Retention</a>.</li></ul>
Change of a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>- Finding no longer appears in the scan findings</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:



Data	Uniqueness Criteria
Asset	id
Finding	cveId + id + deviceId

## API Endpoints in Use

API version: 1.0

API	Use in Tenable Exposure Management	Required Permissions
<a href="https://login.microsoftonline.com/{tenant_id}/oauth2/token">https://login.microsoftonline.com/{tenant_id}/oauth2/token</a>	Authentication for other endpoints	None
<a href="https://api.securitycenter.microsoft.com/api/machines">https://api.securitycenter.microsoft.com/api/machines</a>	Assets	Machine.Read.All Machine.Read
<a href="https://api.securitycenter.microsoft.com/api/machines/SoftwareVulnerabilitiesByMachine">https://api.securitycenter.microsoft.com/api/machines/SoftwareVulnerabilitiesByMachine</a>	Detections, Findings	Vulnerability.Read.All Vulnerability.Read
<a href="https://api.securitycenter.microsoft.com/api/machines/SoftwareVulnerabilityChangesByMachine">https://api.securitycenter.microsoft.com/api/machines/SoftwareVulnerabilityChangesByMachine</a>	Detections	Vulnerability.Read.All Vulnerability.Read

## Data Validation



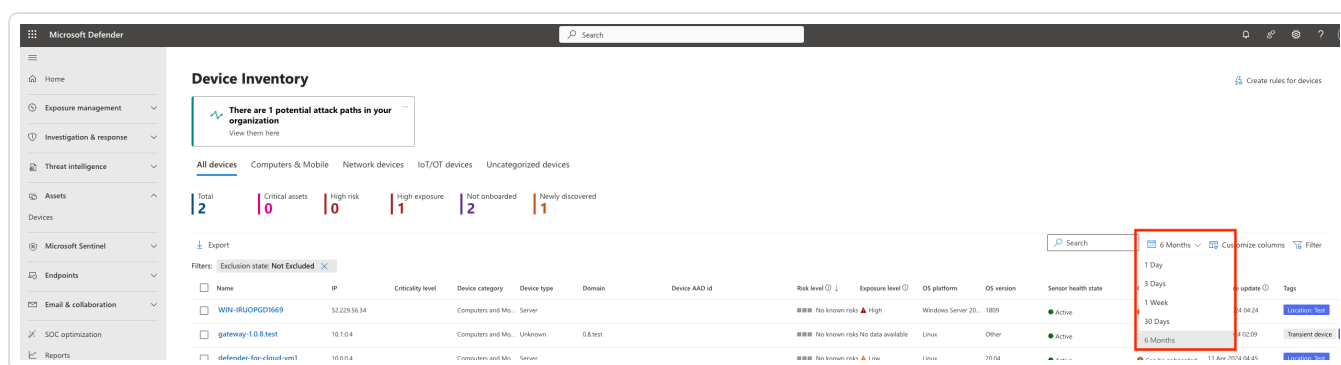
This section shows how to validate and compare data between Tenable Exposure Management and the Microsoft TVM platform.

## Asset Data Validation

**Objective:** Ensure the number of endpoints (devices) in Microsoft TVM aligns with the number of devices displayed in Tenable Exposure Management.

In Microsoft TVM:

1. Navigate to **Assets > Devices**.
2. Set the time filter to the maximum value (6 months).



3. (Optional) Depending on the connector setup in Exposure Management, you may need to apply filters in Microsoft Defender for Vulnerability Management to view the correct set of assets. Apply the following filters based on the connector setup:

- If "**Fetch only onboarded assets**" is enabled, select the **Active** filter in Microsoft Defender for Vulnerability Management.
- If "**Immediately remove assets when their status is set to Inactive is enabled**", exclude the configured value from the filter.



## Data pulling configuration

Set the integration data pulling

☐ Map External IP to Asset

☒ Fetch only Onboarded assets

---

### Asset Retention

Remove assets when their last seen date is more than  days ago

**Immediately remove assets when their status is:**

For example, if **Inactive** is selected in the connector, select **Active** and **Misconfigured** in the Microsoft Defender asset view.



## Filter

 Clear filters

### Sensor health state

- ☐ Active
- ☐ Inactive
- ☐ Misconfigured



### Onboarding status

- ☐ Select all
- ☐ Onboarded
- ☐ Can be onboarded
- ☐ Unsupported
- ☐ Insufficient info

### Antivirus status

- ☐ Select all
- ☐ Disabled
- ☐ Not updated
- ☐ Unknown

### First seen

- ☐ Last 7 days
- ☐ Over 7 days ago

### Tags

### Internet facing

- ☐ No
- ☐ Yes

### Transient device

- ☐ No



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Microsoft TVM and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Microsoft TVM and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on its last observed date (`last_seen` field).
- The asset was archived based on its `healthStatus` value.
- The asset was archived because it did not return in the connector's last sync.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

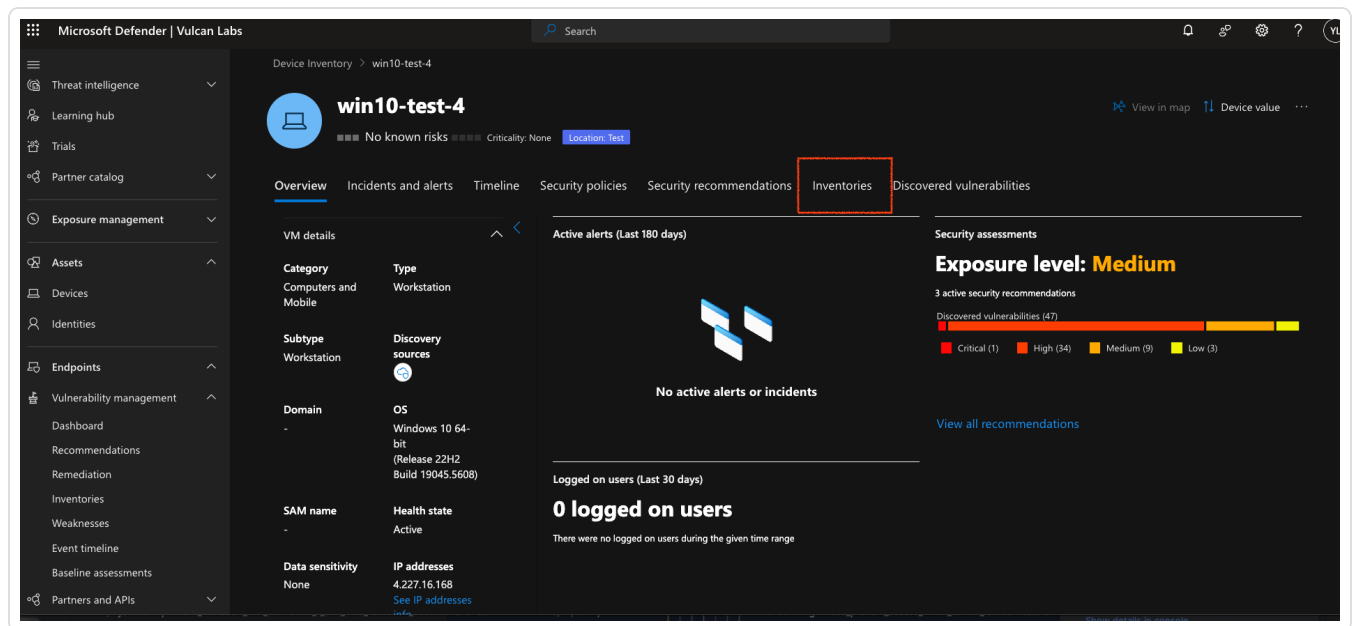
## Finding Data Validation

**Objective:** Ensure the number of findings in Microsoft TVM aligns with the number of findings in Tenable Exposure Management.

In Microsoft TVM:

1. Navigate to **Assets > Devices**.
2. Click on the name of any asset you want to view.
3. Navigate to **Inventories > Software**.





4. Sum up the **Weaknesses** column.

**Tip:** Use the **Export** function to do this efficiently!

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between Microsoft TVM and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Microsoft TVM and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

Outpost24 Connector



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Outpost24](#) Outscan is an automated vulnerability scanner that enables organizations to diagnose, monitor, and triage external vulnerabilities on your internet-exposed devices as well as verify your PCI Compliance for transactional businesses.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Outpost24</a>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Device Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Identify your Outpost Outscan Server URL (e.g., <https://outscan.outpost24.com>)
- **Generate Outpost Credentials:**
  1. Log in to your Outpost24 portal.
  2. Click your account name in the upper-right corner, then select **IAM**.



3. In the **Roles** tab, click **+ Add role**.
4. Name the role Exposure Management or Tenable (or another preferred name).
5. Grant View permissions to:
  - Asset groups
  - Assets



- Findings



## Add role



Name \*

Vulcan

AppStaks™

Deny

View

View and manage

Asset groups

Deny

View

View and manage

Assets

Deny

View

View and manage

Configurations

Deny

View

View and manage

Schedules

Deny

View

View and manage

Scans

Deny

View

View and manage

Findings

Deny

View

View and manage

Compliance

Deny

View

View and manage

Tags

Deny

Manage

Reports

Deny

View and manage

Scheduled reports

Deny

View

View and manage

Managed reports

Deny

View

View and manage

Users

Deny

View

View and manage

Credentials

Deny

View

View and manage

Scoping

Deny

Submit

Dashboards

Deny

View

View and manage

View templates

Deny

View

View and manage

Integrations

Deny

View

View and manage

Events

Deny

View

View and manage

Subscriptions

Deny

View

CORE

Deny

View

- 617 -



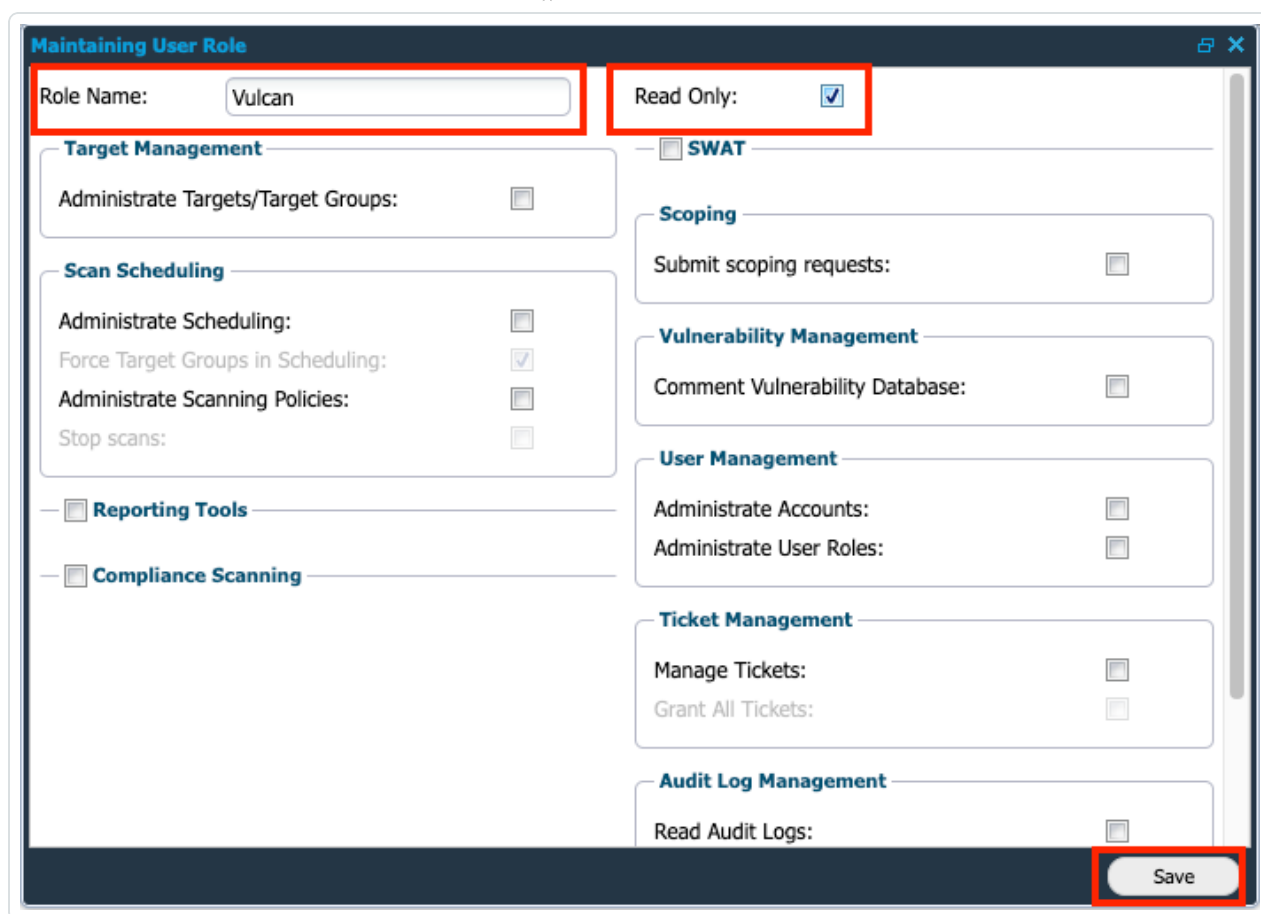
6. Click **Add** to create the role.
7. In the **Users** tab, click **+ Add user**.
8. Fill in the required details:
  - Provide a unique username.
  - Use a valid email address (a temporary password will be sent here).
9. Click **Add**.
10. Retrieve the password from the email. (Optional: log in and update the password.)

- **Assign the Role and Resource Groups:**

1. In the **Users** tab, select the checkbox of the newly created user.
2. Click **Assign roles** and check the role you created earlier.
3. Click **Assign**.
4. Click **Assign resource groups**, select the relevant resource groups, and click **Assign**.

- **Configure NetSec Permissions (Read only):**

1. In the left navigation panel, click **NetSec**.
2. In the bottom-left, click the target icon, then Navigate to: **NetSec > Settings > Manage Users**.
3. In **Manage User Accounts**, navigate to the **User Roles** tab and click **+ New**.
4. Enter the role name you created earlier, check **Read Only**, and click Save.



The image shows a 'Maintaining User Role' dialog box with a dark blue header and a light gray body. The 'Role Name' field is set to 'Vulcan'. The 'Read Only' checkbox is checked. The dialog is divided into two main sections: 'Target Management' and 'Scan Scheduling' on the left, and 'SWAT', 'Scoping', 'Vulnerability Management', 'User Management', 'Ticket Management', and 'Audit Log Management' on the right. Each section contains a list of permissions with checkboxes. The 'Save' button is located at the bottom right.

Section	Permission	Checked
Target Management	Administrate Targets/Target Groups:	<input type="checkbox"/>
	Administrate Scheduling:	<input type="checkbox"/>
Scan Scheduling	Force Target Groups in Scheduling:	<input checked="" type="checkbox"/>
	Administrate Scanning Policies:	<input type="checkbox"/>
	Stop scans:	<input type="checkbox"/>
	Reporting Tools	<input type="checkbox"/>
Compliance Scanning	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
SWAT	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
Scoping	Submit scoping requests:	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability Management	Comment Vulnerability Database:	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
User Management	Administrate Accounts:	<input type="checkbox"/>
	Administrate User Roles:	<input type="checkbox"/>
Ticket Management	Manage Tickets:	<input type="checkbox"/>
	Grant All Tickets:	<input type="checkbox"/>
Audit Log Management	Read Audit Logs:	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>

5. In the **User Accounts** tab, right-click the same user and select Edit.
6. In the Account Settings tab:



- Check **Active**.
- Check the newly created role under **Granted User Roles**.

**Maintaining User Account**

**Account Details**

Parent Account: Top Level

Firstname:

Lastname:

Email: c...@...io

Mobile number:

Country:

State:

Email PGP Public Key: Unencrypted

**Login Details**

Username: Y

Password:

Password again:

Generate Password

2-Factor Authentication: None

☐ Require password change on next logon

**Account Settings** | Granted Targets | Granted SWAT Applications | Attributes

Active: ☒

Super User: ☐

Allow Enroll Hiab: ☐

**Granted User Roles**

☒ Vulcan

7. Navigate to the **Granted Targets** tab and uncheck **Not all Targets Granted**.
8. Navigate to the **Attributes** tab:
  - Enter a value in the Uri\* field (any unique string).
9. Click Save.



**Maintaining User Account**

**Account Details**

Parent Account: Top Level

Firstname:

Lastname:

Email:

Mobile number:

Country:

State:

Email PGP Public Key: Unencrypted

**Login Details**

Username:

Password:

Password again:

Generate Password

2-Factor Authentication: None

☐ Require password change on next logon

Account Settings | Granted Targets | Granted SWAT Applications | **Attributes**

Uri\*: XXX

Save

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

**Connectors** Add new connector

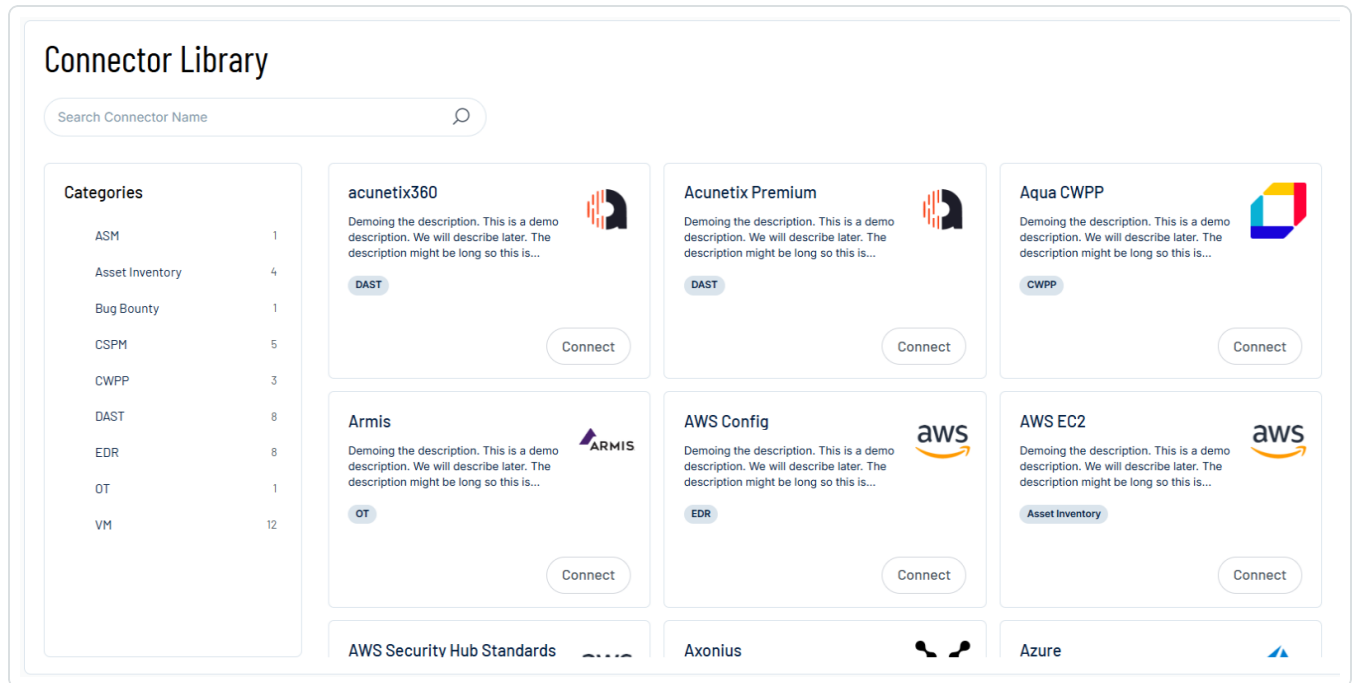
Search Connector Name  Select

Name	Connector type	Status	Last data ingestion	Created on	
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>



2. In the upper-right corner, click **+ Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.
4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server URL** section, type the URL for your Outpost24 server.



4. In the **Username** and **Password** text boxes, paste the user credentials you generated in Outpost24.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - (Optional) To fetch NetSec assets and vulnerabilities from Outpost24, select the **Fetch NetSec assets and vulnerabilities** check box.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

❌ Failed tests 1 out of 4 integration tests failed

✅ Successful tests 3 out of 4 integration tests succeeded

[Test connectivity](#)  
[Show tests](#)   
[Show tests](#)

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).



8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

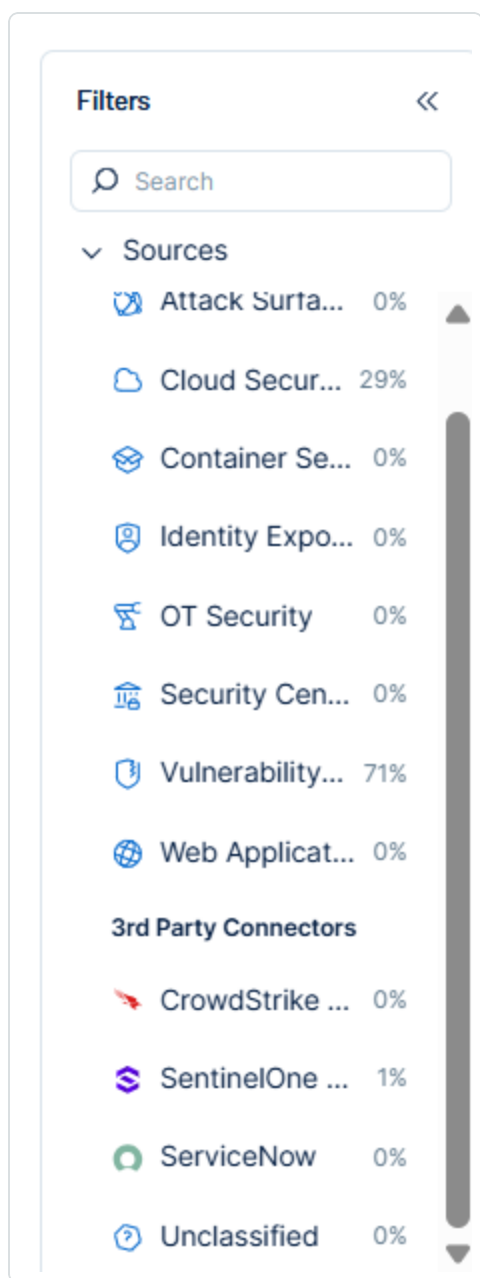
## Outpost 24 in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

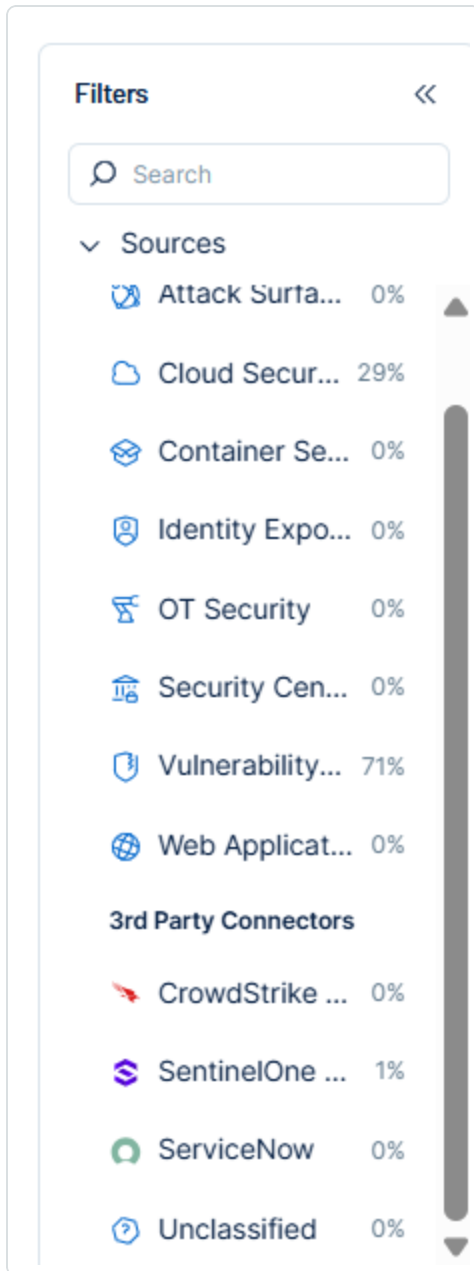
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

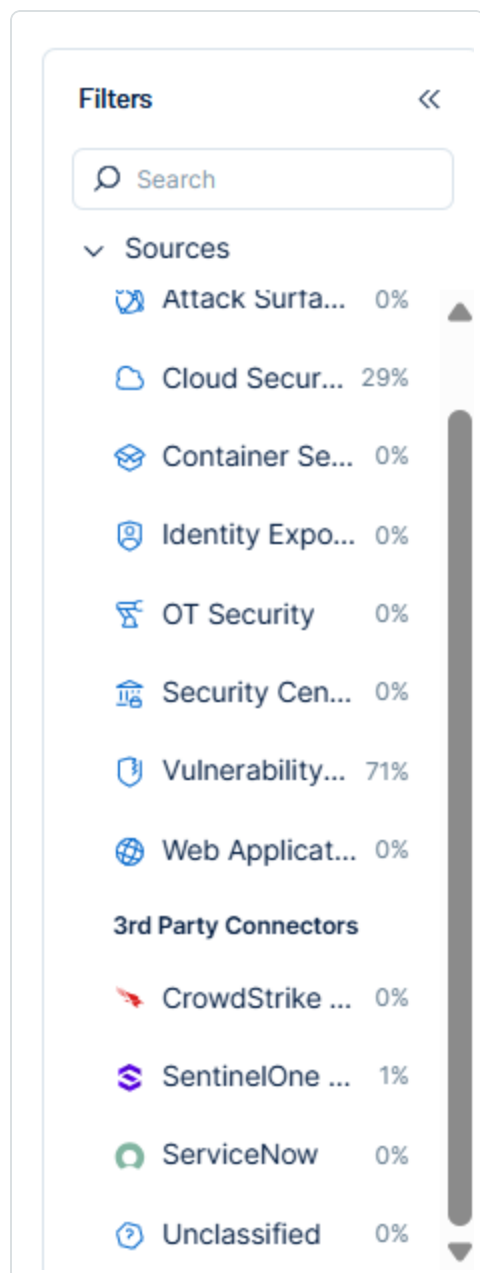
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Outpost24 Field
Unique Identifier	id
Asset - Name	hostname or name
Asset - Operating Systems	os
Asset - First Observation Date	firstSeen or created
Asset - Last Observed At	lastSeen or updated
Asset - External Tags	source businessCriticality exposed assetIdentifiers
Asset Custom Attributes	tags groups

## Finding Mapping (for Device)

Tenable Exposure Management UI Field	Outpost24 Field
Unique Identifier	asset id + id + Unique Vulnerability id





Finding Name	name
CVEs	cve
CWEs	cwe
Severity Driver	nvdCvssV3Score or cvssV3Severity or nvdCvssV2Score
Description	description
Port	port
Protocol	protocol
First Seen	firstSeen or created
Last seen (Observed)	lastSeen
Finding Custom Attributes	packageName or presentableName  vulnId or id  softwareComponent  cyrating  hasExploits  exploitProbability  nvdCvssV3Vector

## Web Application Mapping

Tenable Exposure Management Value	Outpost24 Value
Unique Identifier	id
Asset - Name	name
Asset - First Observation Date	firstSeen or created
Asset - Last Observed At	lastSeen or updated



Asset - External Tags	tags groups
Asset Custom Attributes	source asset_identifiers

## Finding Mapping (for Web Application)

Tenable Exposure Management UI Field	Outpost24 Field
Unique Identifier	asset id + match id + Unique Vulnerability id
Finding Name	name
CVEs	cve
CWEs	cwe
Severity Driver	nvdCvssV3Score or cvssV3Severity or nvdCvssV2Score
Description	description
First Seen	firstSeen or created
Last seen (Observed)	lastSeen
Finding Custom Attributes	url source port protocol id softwareComponent cyrating hasExploits



	exploitProbability
	nvdCvssV3Vector

## Finding Status Mapping

Tenable Exposure Management Status	[Connector] Status
Active	PRESENT  isAccepted:false (for NetSec)  FALSE_POSITIVE  IRREPRODUCIBLE  REJECTED  ACCEPTED  isAccepted:true (for NetSec)  TO_PUSH  TO_QA  PENDING_VERIFICATION  TO_REVIEW  TO_VERIFY
Fixed	FIXED

**Note:**For Outpost24, Exposure Management uses the findings\_status field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	[Connector] Score
Critical	<b>CVSS:</b> 9.0 - 10.0  <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9



	<b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:** For Outpost24, Exposure Management uses the `nvdCvssV3Score` or `cvssV3Severity` or `nvdCvssV2Score` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <code>findings_status = FIXED</code> on the vendor side]</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).



## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Finding	asset id + id + Unique Vulnerability id
Detection	Website / cloud resource: checkId Host: vulnId
Solution	solutionUuid

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Discrepancy in Asset Visibility Between Outpost24 Portal and Tenable

Some customers use the NetSec module in Outpost24, which includes host data collected from agents running on machines. In these cases, certain hosts may appear in NetSec but not in the Outpost24 Portal interface.

The Exposure Management connector ingests data from both the Portal and NetSec, which may result in assets appearing in Exposure Management that are not visible in the Outpost24 Portal.

### Apparent Asset Duplication in Tenable



Outpost24 does not differentiate between asset types (e.g., devices vs. web applications). As a result, it may represent multiple asset types as a single entity.

Exposure Management, however, distinguishes between asset types. This difference may lead to apparent duplication of assets in Exposure Management.

Example:

If an Outpost24 agent is installed on a machine that also hosts a web application:

- Outpost24 displays this as a single asset.
- Exposure Management displays two distinct assets: one as a device, and another as a Web Application.

This behavior is expected and results from Exposure Management granular asset classification model.

## API Endpoints in Use

API version: v1.0

API	Use in Tenable Exposure Management	Required Permissions
/opi/rest/auth/login	Token generation	None
/opi/rest/outscan/targets	Assets (devices)	Read Only for all targets
/opi/rest/outscan/findings	Findings, Assets enrichment	Read Only for all targets
/opi/rest/checks	Detections	View Findings
/opi/rest/assets	Assets (Web applications)	View Assets
/opi/rest/findings	Findings	View Findings
/opi/rest/matches	Findings	View Findings
/opi/rest/checks	Detections	View Findings
/opi/rest/asset-groups	Asset enrichment (tags)	View Asset Groups



## Data Validation

This section outlines how to validate and compare data between Exposure Management and the Outpost24 platform.

### Asset Data Validation

**Objective:** Ensure that the number of assets in Outpost24 aligns with the number of assets displayed in Tenable Exposure Management.

In Outpost24:

1. Navigate to the **Assets** section and select the **Assets** tab.
2. Apply a filter on the **Source** column based on asset type:
  - Select **NETSEC** and **VERIFY** to view device assets.
  - Select **CLOUDSEC** to view resources.
  - Select all other sources (excluding the above) to view web applications.
3. At the top of the list, select the checkbox next to **Name** to highlight all items.
4. At the bottom of the screen, review the total number of filtered assets.

**Note:** Some customers use the NetSec module, which includes agents running on machines. These hosts may not appear in the Portal but are ingested into Exposure Management. Exposure Management displays all NetSec and Portal data sources, which may lead to a higher asset count.

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Outpost24 and Tenable Exposure Management.

**Expected outcome:** Asset counts may not align exactly due to Outpost24 grouping multiple asset types under a single entry, whereas Exposure Management separates these into distinct asset types (for example, device vs. web application).

If an asset is not visible in Exposure Management, check the following conditions:



- The asset was archived based on the last observed date (last seen).
- The asset was archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the number of findings in Outpost24 aligns with the number of findings displayed in Exposure Management.

In Outpost24 Portal:

1. Navigate to the **Assets** section and select the **Assets** tab.
2. Apply a filter on the **Source** column based on asset type:
  - Select **NETSEC** and **VERIFY** to view device assets.
  - Select **CLOUDSEC** to view resources.
  - Select all other sources (excluding the above) to view web applications.
3. Select the checkbox next to **Name** for all applicable assets.
4. At the bottom of the screen, click **Generate Report**.
5. In the wizard:
  - Select the **Vulnerabilities** report type.
  - Choose **Detailed**.
  - Uncheck **PDF** and select **Excel format**.
  - Choose **Custom date range** from 1999-01-01 to the current date.
6. Download the generated Excel file from the cloud icon.
7. Open the **Risk Details** sheet to view all findings.

In Outpost24 NetSec:





1. Navigate to **NetSec > Reporting Tools**.
2. Select the relevant **Target Group** (e.g., All Targets).
3. Click **Export Report**.
4. Set:
  - Format: **Excel**
  - Report Type: **Vulnerability**
  - Target Summary: **All Selected Targets**
5. Download and open the file.
6. Review the **Vulnerability Details** sheet to see all findings.

In Tenable Exposure Management:

1. [Locate your connector findings](#).
2. Compare the total number of findings between Outpost24 and Tenable Exposure Management.

**Expected outcome:** Finding counts may differ slightly due to data granularity or filtering differences. Outpost24 may present one asset with multiple findings collapsed, whereas Exposure Management separates them per asset and source.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

PrismaCloud CWPP Connector



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Prisma Cloud \(Palo Alto Networks\)](#) is a comprehensive Cloud Workload Protection solution that delivers flexible protection to secure cloud VMs, containers and Kubernetes apps, serverless functions and containerized offerings like AWS Fargate® tasks. With Prisma Cloud, DevOps and cloud infrastructure teams can adopt the architecture that fits their needs without worrying about security keeping pace with release cycles or protecting a variety of tech stacks.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Prisma Cloud (Palo Alto Networks)</a> Compute Edition (self-hosted) and Enterprise Edition v.20.04 or the cloud version
Category	CWPP
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices Containers
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:



- **Identify the Prisma Cloud CWPP server URL:**

1. Navigate to **Runtime Security > Manage > System**.
2. Click on **Utilities**.
3. Identify the server URL.

- **Assign a System Administrator role for full access, or configure a custom role:**

- Assign the role to a specific **Account Group** that includes the resources to be synced (e.g., cloud accounts or on-premises Kubernetes clusters).

**Create New Role** ×

Name  
name

Description (Optional)  
description

Permission Group [View Permissions](#)  
Account Group Read Only

Account Group (Optional)  
Default Account Group

- If you plan to ingest data from on-premises Kubernetes clusters, select the **On-Prem / Other Cloud Providers** checkbox in the **Advanced Options** section of the role configuration.
- Confirm that the **Account Group** is not empty and contains the required resources.

- **Generate PrismaCloud CWPP Access and Secret Keys:**



**Note:** These should be the credentials of a valid Prisma Cloud user with the assigned role as described above.

1. Sign in to the Prisma Cloud console.
2. Navigate to **Settings > Access Control > Users**.
3. Create a new user or select an existing one.
4. Assign the appropriate role and account group.
5. Ensure that the API key **Expiration** is set to within **6 months** of the generation date.
6. Generate an **Access Key ID** and **Secret Key** for the user.
7. Save the credentials securely. You'll use them to configure the connector in Exposure Management.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

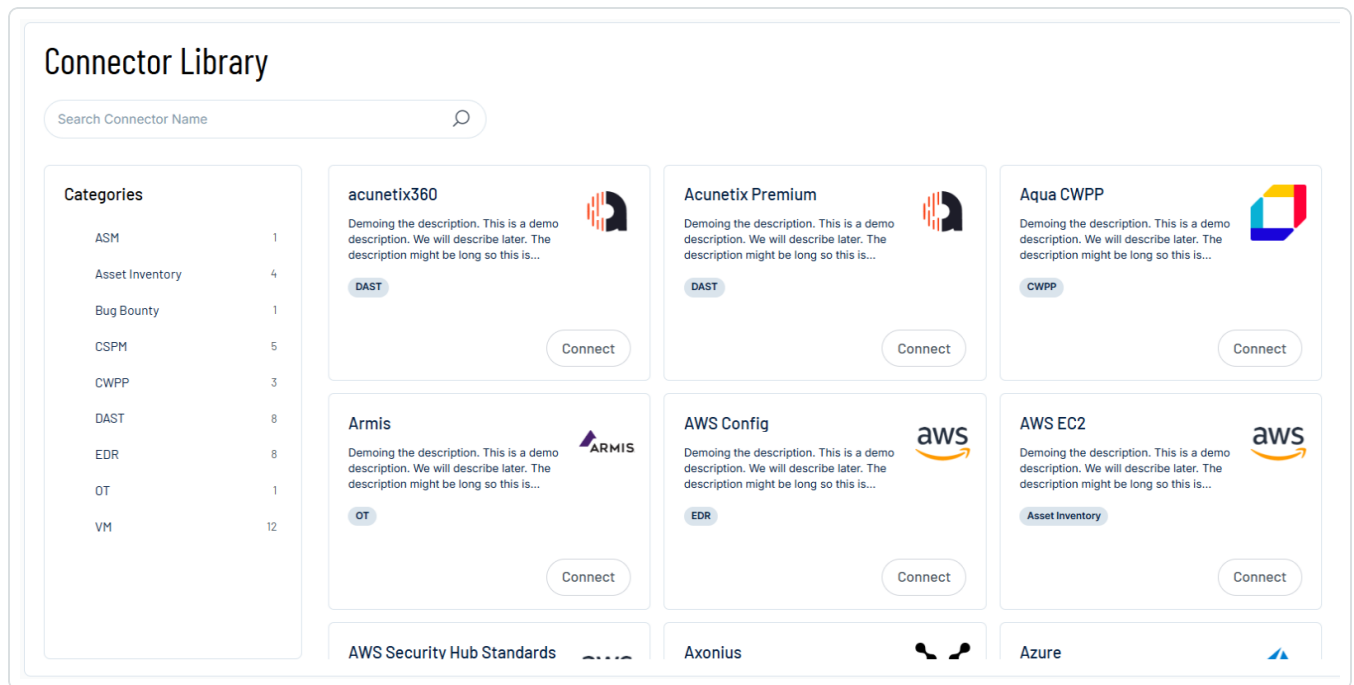
The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

2. In the upper-right corner, click **Add new connector**.



The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server Url** section, type the URL of your PrismaCloud server.
4. In the **Access Key ID** and **Secret Access Key** text boxes, paste the secret credentials you generated in PrismaCloud.



5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.

- In **PrismaCloud Assets**, check the assets you want to fetch:
  - **Fetch Hosts**: Mapped as Devices in Exposure Management
  - **Fetch Images**: Mapped as Containers in Exposure Management
  - **Fetch CI Images**: Mapped as Containers in Exposure Management
  - **Fetch Registries**: Mapped as Containers in Exposure Management
- In **Vulnerabilities**, check the "**Base image indication for Image vulnerabilities**" if relevant.
- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.

- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

Show tests ▾

**Successful tests** 3 out of 4 integration tests succeeded

Show tests ▾



7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

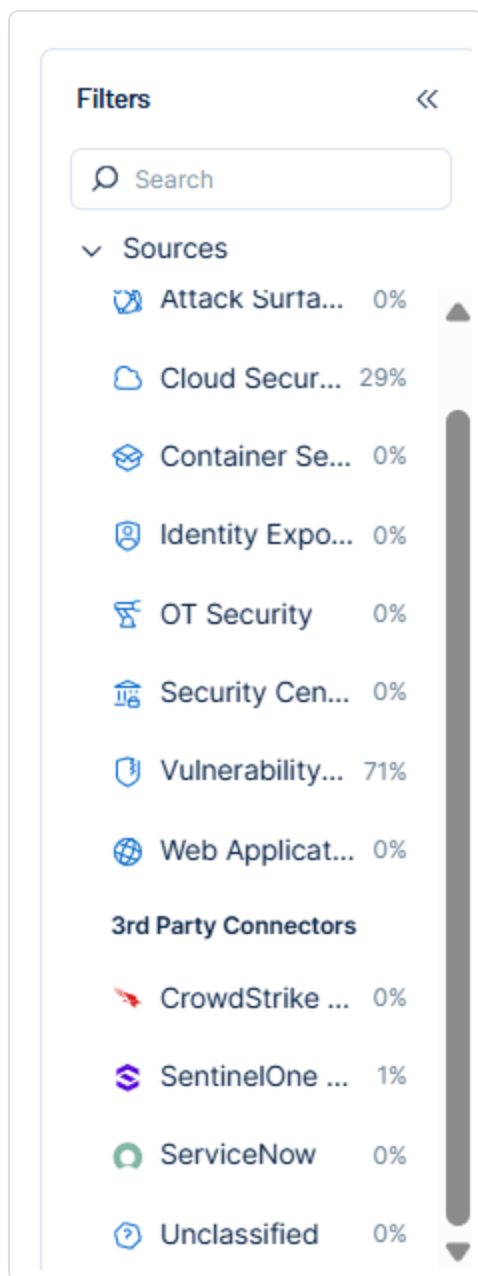
## Prisma CWPP in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Locate Connector Weaknesses in Tenable Exposure Management

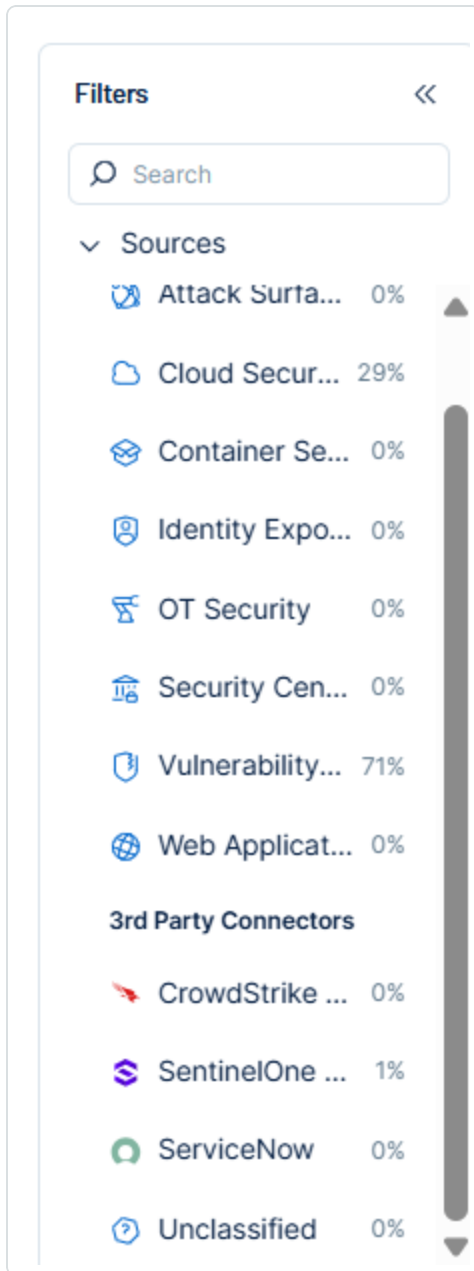
As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:





1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

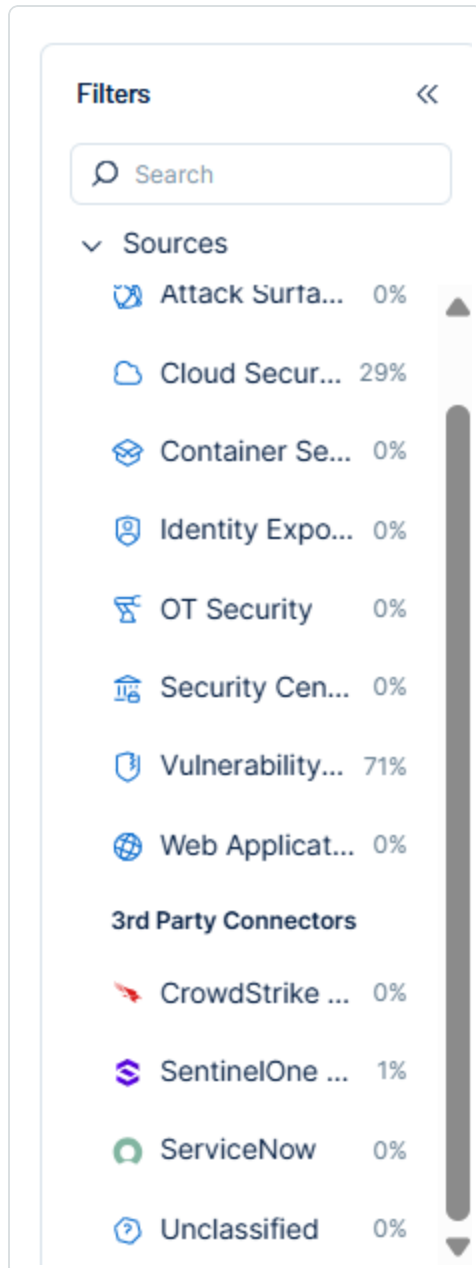
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Prisma CWPP Field
Unique Identifier	<code>_id</code>
Asset - External Identifier or Asset - Provider Identifier	<code>cloudMetadata.resourceID</code>
Asset - Name	<code>hostname</code>
Asset - Operating Systems	<code>distro</code> <code>osDistro</code>
Asset - OS Version	<code>osDistroVersion</code>
Asset - IPv4 Adresses Asset - IPv6 Adresses	<code>hostDevices</code>
Asset - First Observation Date	<code>firstScanTime</code>
Asset - Last Observed At	<code>scanTime</code>
Asset - External Tags	<code>tags</code>
Asset Custom Attributes	<code>Docker Version</code> <code>Host Id</code> <code>Account Id</code>

## Finding Mapping (for Devices)



Tenable Exposure Management UI Field	Prisma CWPP Field
Unique Identifier	cve + packageName + packageVersion
Finding Name	title or text or cve
CVEs	cve
Severity Driver	cvss
Risk Factor	
Description	description
Last seen (Observed)	discovered
Finding Custom Attributes	packageName packageVersion severity cvss vecStr

## Container Mapping

Tenable Exposure Management UI Field	Prisma CWPP Field
Unique Identifier	_id
Asset - Name	_id
Asset - Operating Systems	distro or osDistro
Asset - OS Version	osDistroVersion
Asset - Container Image Tags	repoTag.tag
Asset - Image Digest	_id or repoTag=digest
Asset - First Observation Date / Created Date	firstScanTime



Asset - Last Observed At	scanTime
Asset - External Tags	tag_list
Asset Custom Attributes	Account Id- cloudMetadata.accountID Collections- collections Err - err Prismacloud Id - _id Registry - instances.registry Scan Version - scanVersion Trust Status - trustStatus

## Finding Mapping (for Containers)

Tenable Exposure Management UI Field	Prisma CWPP Field
Unique Identifier	cve + packageName + packageVersion
Finding Name	title or text or cve
CVEs	cve
Severity	cvss
Severity Driver	
Risk Factor	
Description	description
Last seen (Observed)	discovered
In case a finding is fixed, then > Findings > Last Fixed At	
Finding Custom Attributes	vecStr packageName



	<code>packageVersion</code>
	<code>packageType</code>
	<code>cvss</code>
	<code>severity</code>

## Finding Status Mapping

Tenable Exposure Management Status	Prisma CWPP Status
Active	Findings returned in the current API response
Fixed	Findings that no longer appear in the API response during connector sync

## Finding Severity Mapping

Tenable Exposure Management Severity	Prisma CWPP Score
Critical	<b>CVSS:</b> 9.0 - 10.0
High	<b>CVSS:</b> 7.0 - 8.9
Medium	<b>CVSS:</b> 4.0 - 6.9
Low	<b>CVSS:</b> 1-3.9
None	<b>CVSS:</b> 0

**Note:**For Prisma CWPP, Exposure Management uses the `cvss` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.



Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	Asset not seen for X days according to "Last Seen" See <a href="#">Asset Retention</a>
Change a Finding status from "Active" to "Fixed"	Finding no longer appears in the scan findings

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Finding	cve + packageName + packageVersion
Detection	cve

## API Endpoints in Use

API version: v1.0, v34.00

/api/v1/hosts	
/api/v1/images	
/api/v1/registry	
/api/v1/scans	Assets (Containers)



## Purplemet Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Purplemet](#) is a Web Application Security Monitoring SaaS solution focused on what hackers may see and exploit. It's complementary to scanners enabling cyber hygiene on a URL portfolio while providing an additional list of vulnerabilities and technologies that makes Purplemet the fastest, most cost-effective, and the non-intrusive benchmark solution for web app security.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">Purplemet</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

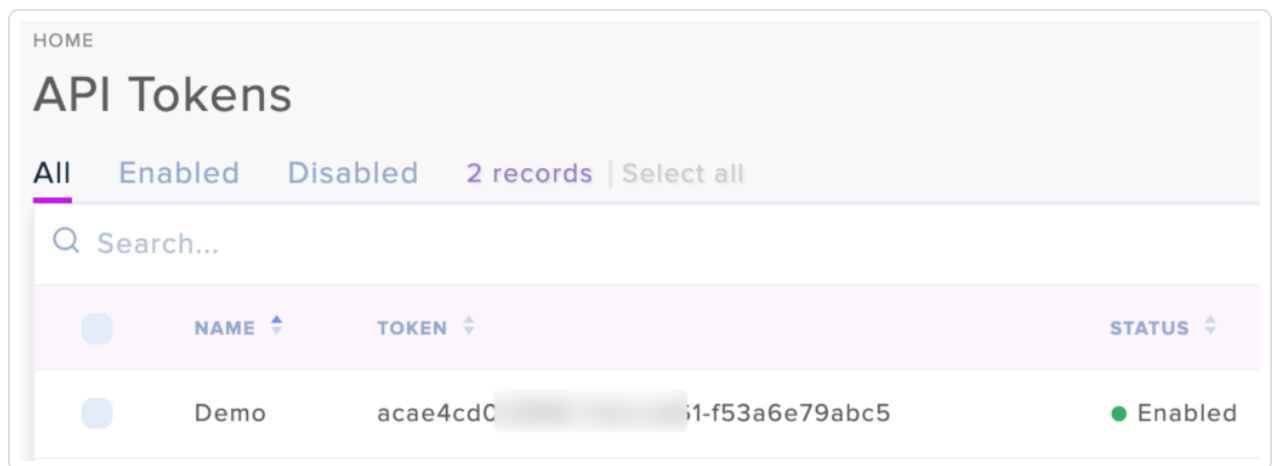
### Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:





- Verify your Purplemet subscription is active.
- **Generate a Purplemet API Key:**
  1. Navigate to your Purplemet platform.
  2. In the left menu, click **Tokens**.
  3. Click **Add**.
  4. Type a **Friendly Name** (for example, ExposureManagementAPI) and enable the **Activation** toggle.
  5. Click **Generate**.
  6. In the upper-right corner, click **Confirm**.
  7. Ensure the status of the generated API token is **Enabled**.



## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

- 654 -



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Key** text box, paste the API key you generated in Purplemet.
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- For the **Immediately remove assets when their status is** option, choose to automatically remove assets that reach a certain asset status, for example, **terminated**.
5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
    - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
    - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

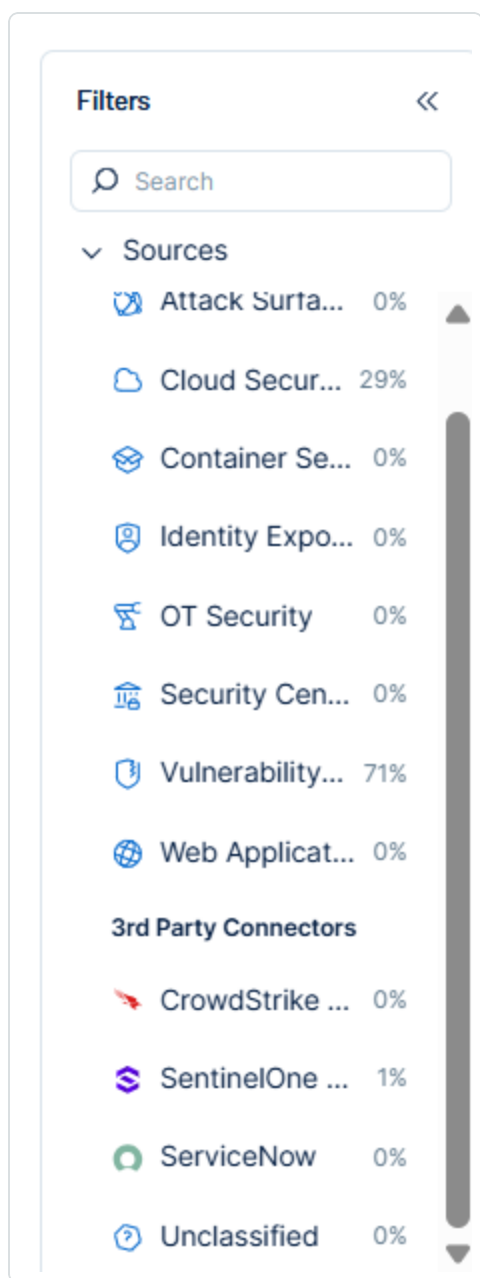
## Purplemet in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

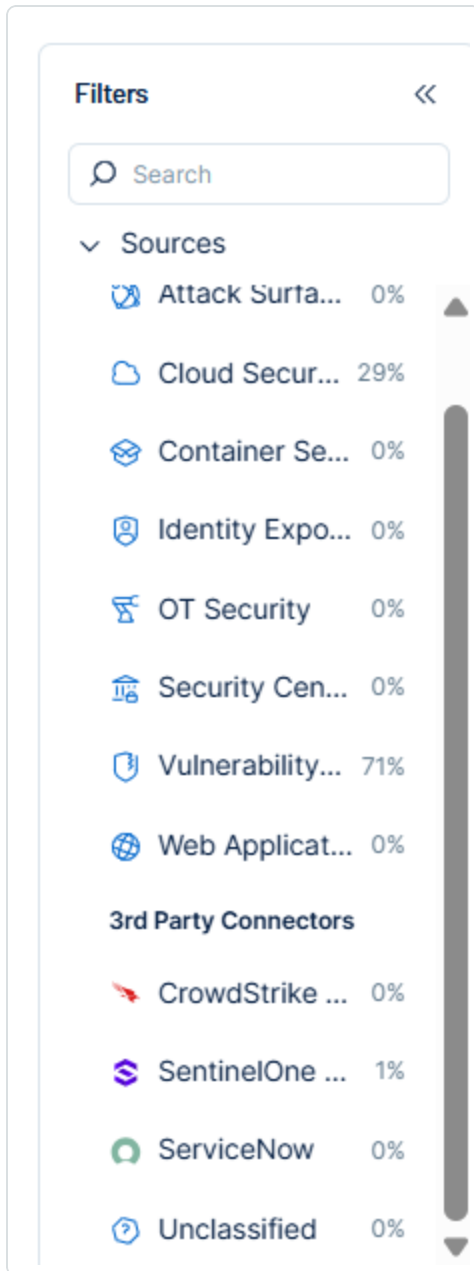
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

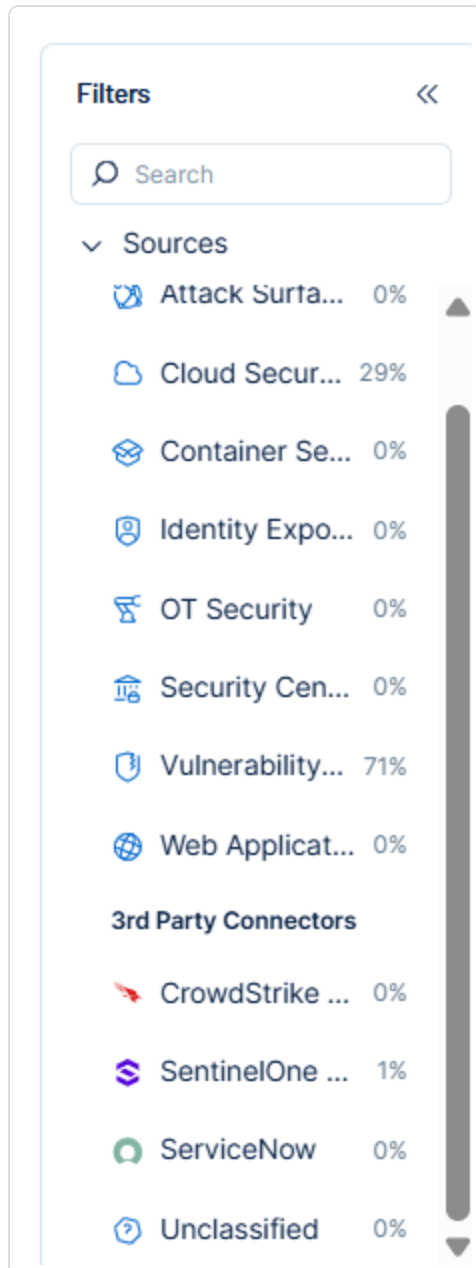
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management Value	Purplemet Value
Unique Identifier	Web application ID
Asset - Name	Web application URL
Asset - First Observation Date	createdAt
Asset - Last Observed At	lastAnalysisDate
Asset - Webapp Homepage Screenshot Url	Web application URL
Asset - External Tags	Tags
Asset Custom Attributes	Web application ID IP address Number of technologies Rating notification enabled last analysis status last analysis mode last analysis user name

## Finding Mapping





Tenable Exposure Management UI Field	Purplemet Field
Unique Identifier	Issue name + Web application URL
Finding Name	Issue name
CVEs	CVEs
Severity Driver	severity cvss3_scoring cvss3_severity
Description	data.description
First Seen	firstDetectedAt
Last seen (Observed)	lastDetectedAt
Finding Custom Attributes	issue_type technology_name technology_version reference cwe_name severity score cvss3_vector Issue ID

### Finding Status Mapping

Tenable Exposure Management Status	Purplemet Status
Active	Open Ignored
Fixed	Fixed



**Note:**For Purplemet, Tenable uses the `status` field to determine status.

## Finding Severity Mapping

Tenable Exposure Management Severity	Purplemet Score
Critical	<b>Severity:</b> Critical
High	<b>Severity:</b> High
Medium	<b>Severity:</b> Medium
Low	<b>Severity:</b> Low

**Note:**For Purplemet, Tenable uses the `severity` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Exposure Management and is not returned on the next connector sync</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <b>fixed</b> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria



Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	Web application ID
Finding	Issue name + Web application URL

## API Endpoints in Use

API version: v1.15.4

<a href="https://api.purplemet.com/site">https://api.purplemet.com/site</a>	
<a href="https://api.purplemet.com/site/tag">https://api.purplemet.com/site/tag</a>	
<a href="https://api.purplemet.com/site/{tag_id}/site">https://api.purplemet.com/site/{tag_id}/site</a>	
<a href="https://api.purplemet.com/issue">https://api.purplemet.com/issue</a>	Findings

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Purplemet platform.

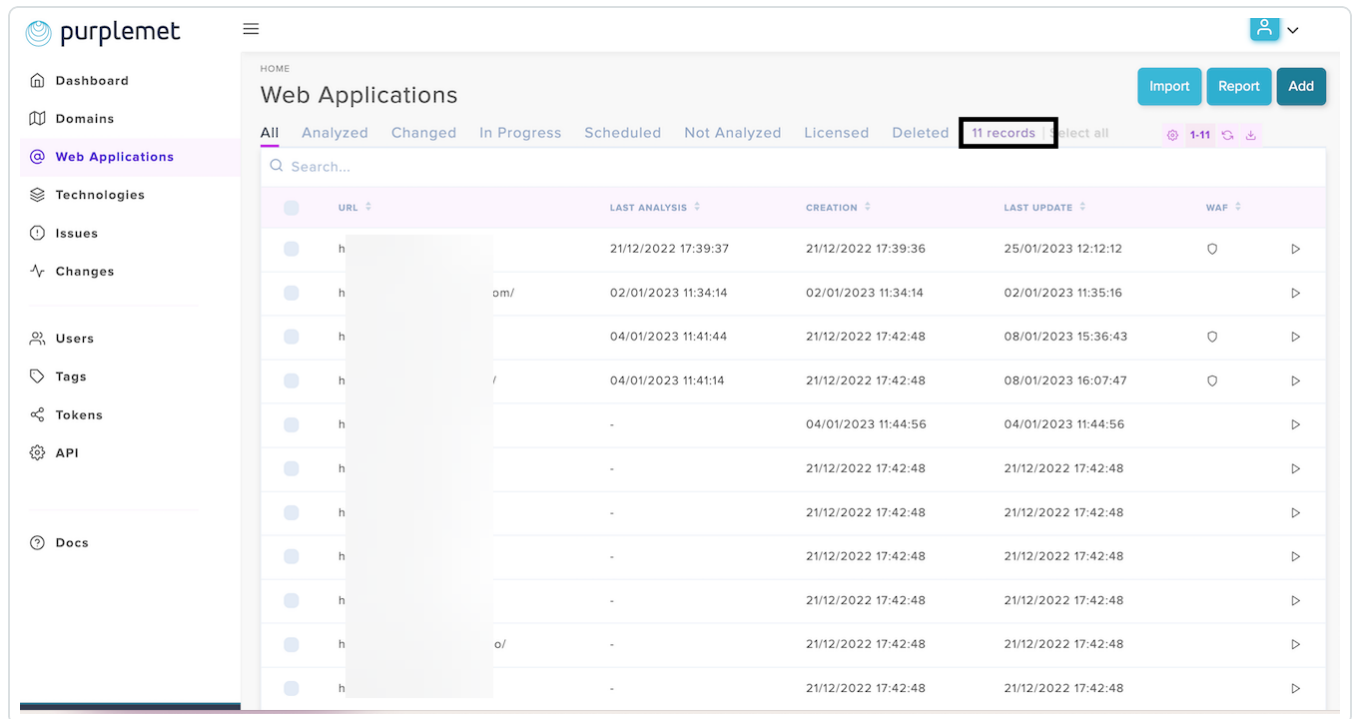
### Asset Data Validation

**Objective:** Ensure the number of web applications in Purplemet aligns with the assets displayed in Tenable Exposure Management.

In Purplemet:



1. Navigate to **Web Applications** from the left navigation menu.
2. Review the list of websites. This list represents all web applications discovered in the tenant.



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Purplemet and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Purplemet and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [Purplemet Connector](#).

## Finding Data Validation

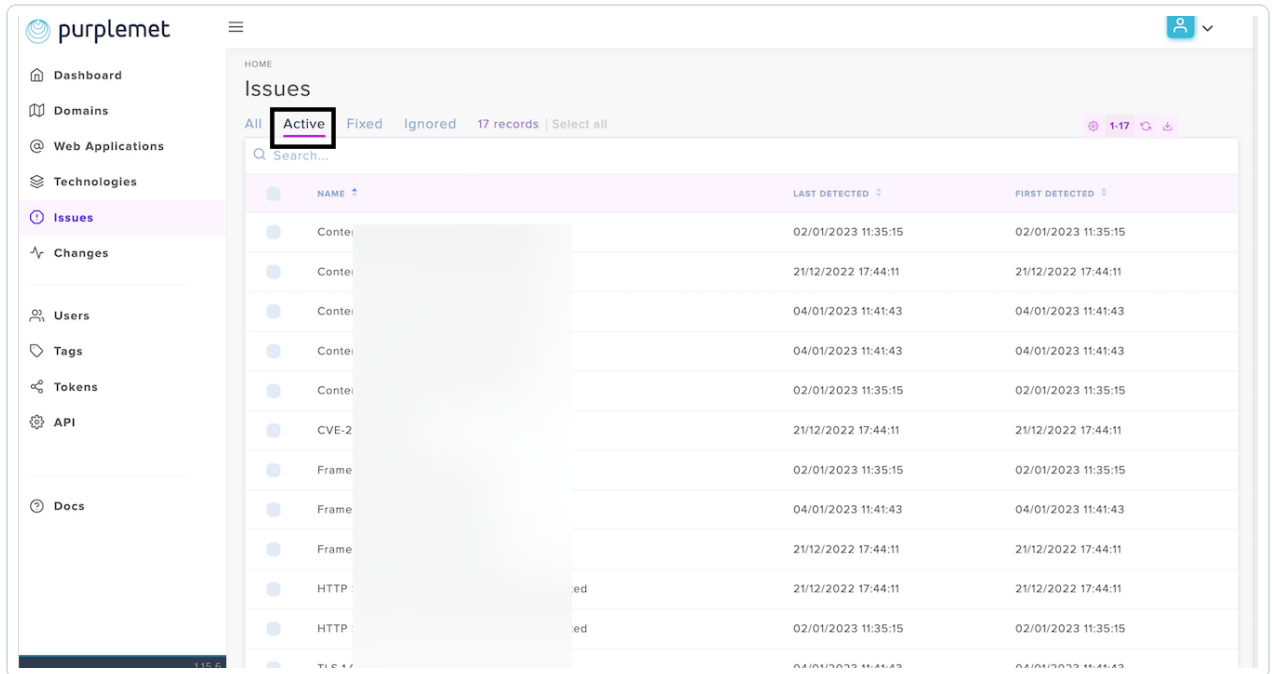
**Objective:** Ensure the number of vulnerability instances in Purplemet aligns with the findings displayed in Tenable Exposure Management.



In Purplemet:

1. Navigate to **Issues**.

- Purplemet displays issues individually per asset, meaning the same vulnerability may appear multiple times across different assets.
- Make sure the **Active** tab is selected when comparing active vulnerabilities. Purplemet view also includes Fixed and Ignored statuses.



In Tenable Exposure Management:

1. [Locate your connector findings](#).
2. Compare the total number of findings between Purplemet and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Purplemet and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.



**Tip:** To learn more on how assets and findings are archived or change status, see [Purplemet Connector](#).

## Qualys Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Qualys](#) provides cloud-based cybersecurity solutions designed to help organizations assess vulnerabilities, manage assets, enforce compliance, secure web applications, protect cloud environments, and automate security processes, enhancing their overall cybersecurity posture and resilience against cyber threats.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">Qualys</a>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Device
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

### Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:



- Identify your Qualys API Server URL (based on region and platform).

- **Create Qualys Credentials (User Role and Permissions):**

1. Click **User Role**, and assign the **Scanner** role to the user.
2. Enable access to **GUI** and **API**.

**User Role**

User Role: \* Scanner

Allow access to: ☒ GUI ☒ API

Business Unit: \* Unassigned

[New Business Unit](#)

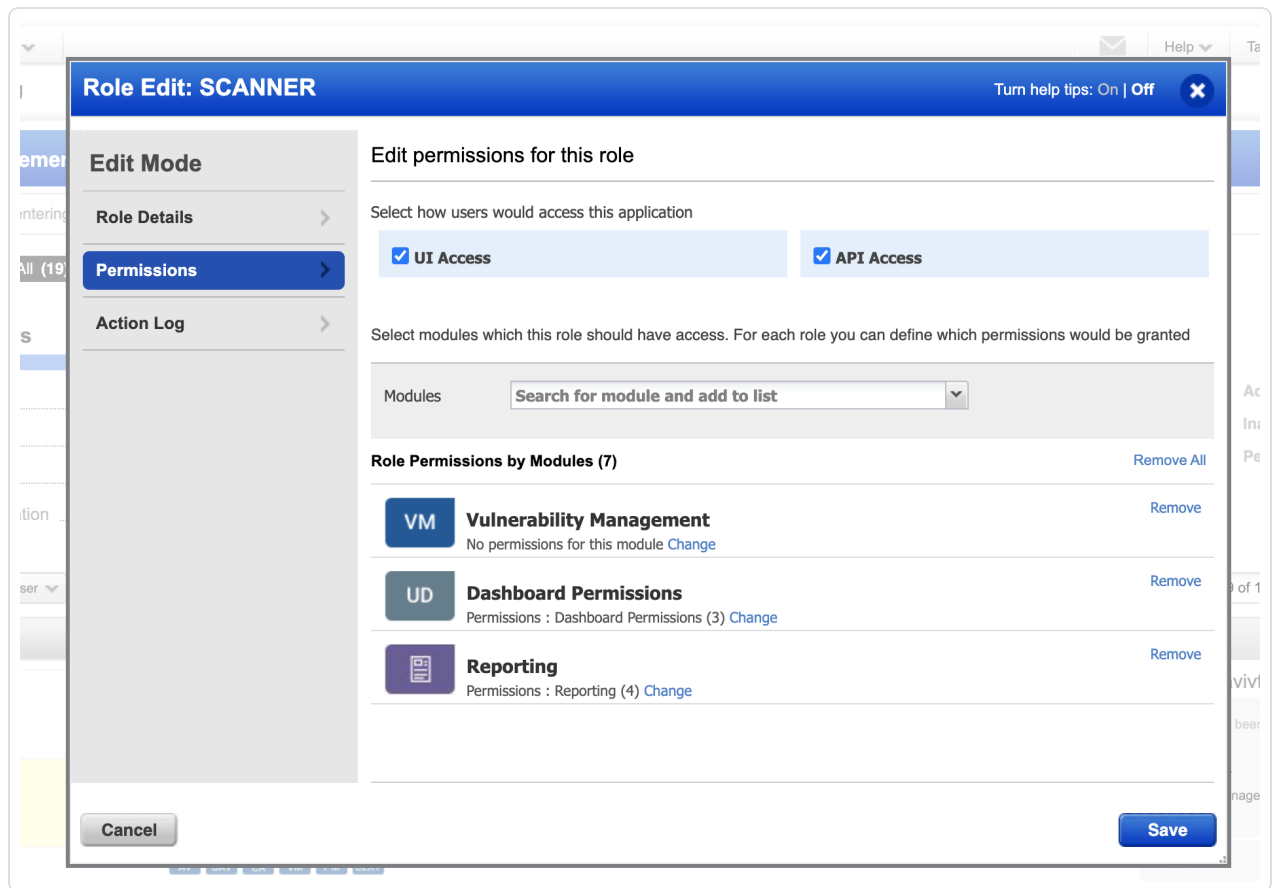
**User configurations to transfer:**

Changing the user's business unit or user role will result in the **removal of personal configurations and asset groups from the user**. Select the options below if you wish to transfer those configurations and asset groups to the user's Manager/Unit Manager. [Learn more](#)

☐ Transfer personal configurations  
Includes option profiles, report templates, scheduled tasks, distribution groups, search lists, web applications and compliance policies.

☐ Transfer Asset Groups  
If not selected, configurations may become inactive (e.g. report templates, schedules) and you'll need to manually update them.

3. Click **Asset Groups** and assign the relevant asset groups to the user.
4. Click **Save** to create the user.
5. Once the user appears in the user list, click the user entry to open their details.
6. Under the **Scanner** role, ensure that both **API** access and **GUI** access permissions are selected.



7. In the Modules drop-down, select **Manage PC Module** and enable the following permissions:

- a. **Manage VM Module**
- b. **Manage PC Module**

8. Click **Save** to add the module to the user permissions.

9. Complete the user creation and save the generated credentials somewhere safe (user name and password).

#### • **Enable Qualys CVSS Scoring:**

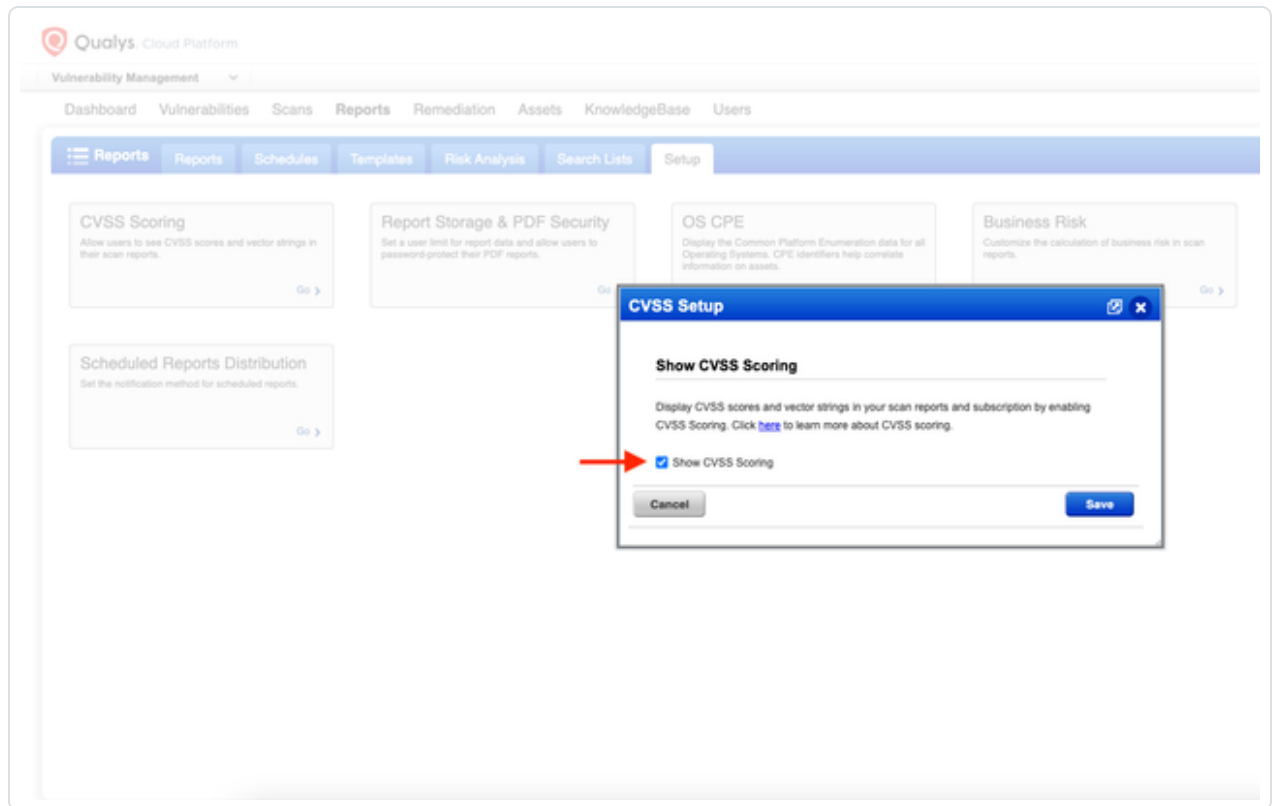
[CVSS scoring](#) is not enabled by default in Qualys. To ensure vulnerability scores are available in Exposure Management, you must enable this feature in your Qualys environment.

To enable CVSS scoring:





1. Log in to your Qualys account.
2. Navigate to the **Reports** tab.
3. Select the **Setup** tab.
4. Click **CVSS** Scoring.
5. Check the box labeled **Show CVSS Scoring**.



6. Click **Save**.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Server Url** drop-down, select the appropriate server URL to use for API configuration.
4. In the **Username** and **Password** text boxes, paste your Qualys client credentials.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - Use the **ark\_kernel\_filter** drop-down to filter vulnerabilities related to the system kernel. This filter helps exclude vulnerabilities that may have already been remediated but are still linked to outdated kernel versions that remain installed.

**Note:** Exposure Management disregards this filter when importing fixed vulnerabilities. This is intentional—Exposure Management continues tracking when a vulnerability was resolved, even if the vulnerable kernel is no longer active.

Select one of the following options:

- **Vulnerabilities related to the kernel are not filtered based on kernel activity.** This matches the default configuration in Qualys, meaning vulnerabilities related to the kernel are not filtered based on kernel activity.
- **Exclude kernel-related vulnerabilities that are not exploitable** (found on non-running kernels).
- **Include only kernel-related vulnerabilities that are not exploitable** (found on non-running kernels).



- **Include only kernel-related vulnerabilities that are exploitable** (found on running kernels).
- From the **Subscription type** drop-down, select the subscription type of your Qualys account.
- (Optional) Enable the **Fetch Potential vulnerabilities** option to ingest potential vulnerabilities identified by Qualys. Select this option if your organization wants broader visibility into possibly vulnerable systems, even if the vulnerability hasn't been confirmed through direct detection.

**Note:** Potential vulnerabilities are detections based on indirect evidence (e.g., version-based or inferred) rather than confirmed exploit presence. Enabling this setting increases visibility but may introduce additional noise in the findings.

- (Optional) Enable the **Fetch Superseded QIDS** to ingest superseded QIDs (Qualys IDs). Enable if your organization wants to track historical detection coverage or if you're working with legacy remediation workflows where superseded QIDs are still relevant.

**Note:** Superseded QIDs are older detections that have been replaced by newer signatures in Qualys. Enabling this setting includes them in the findings ingested into Exposure Management.

- (Optional) In the **Tags** text box, type a list of comma separated tags to apply to the ingested Qualys data.
- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) From the drop-down menu, you can choose to automatically remove assets that reach a certain asset status, for example, **TERMINATED**.

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.



- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

**Successful tests** 3 out of 4 integration tests succeeded

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Qualys in Tenable Exposure Management

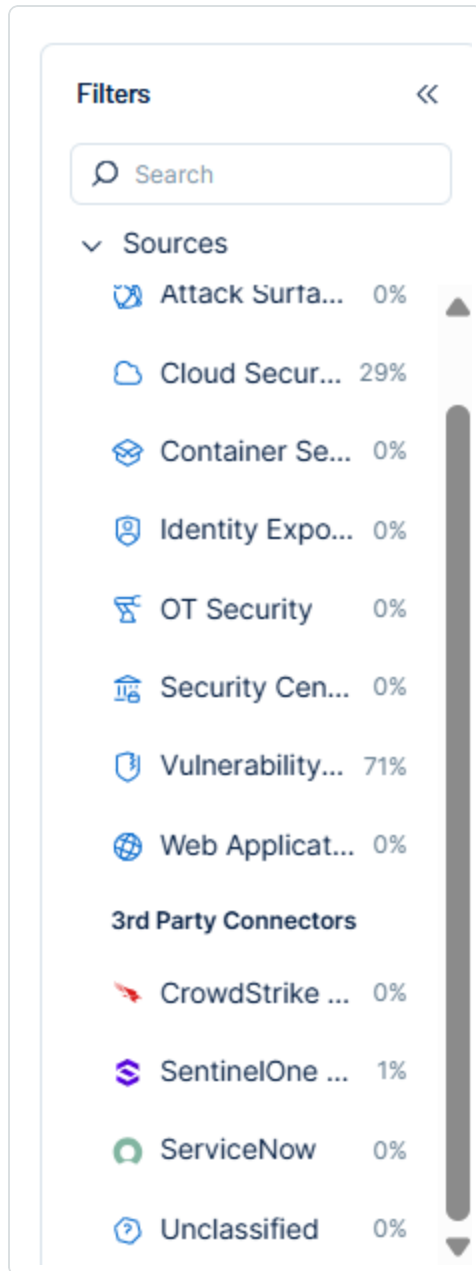
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

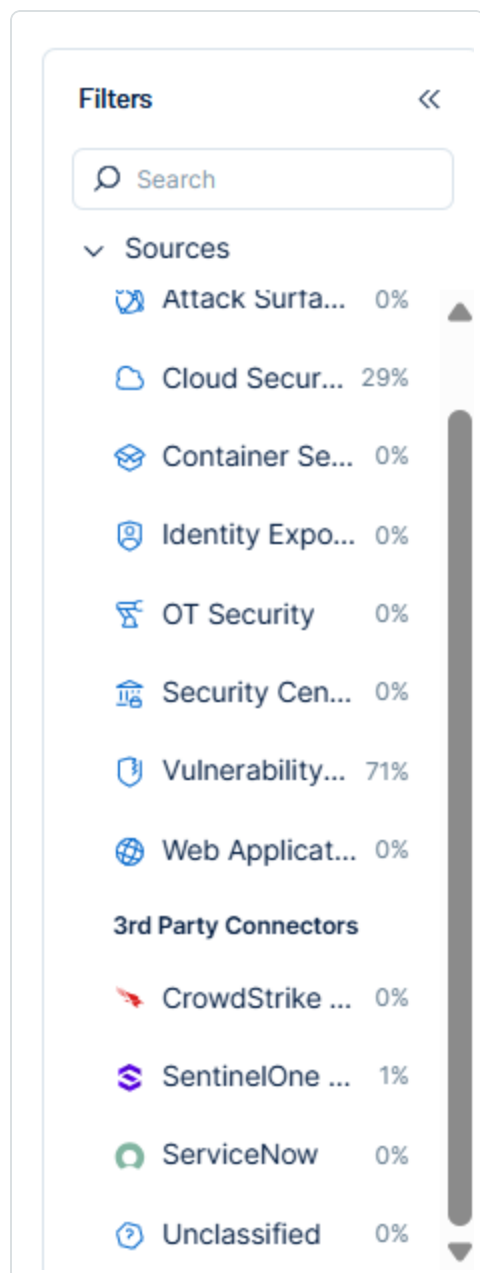
## Locate Connector Weaknesses in Tenable Exposure Management



As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:

1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.





The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

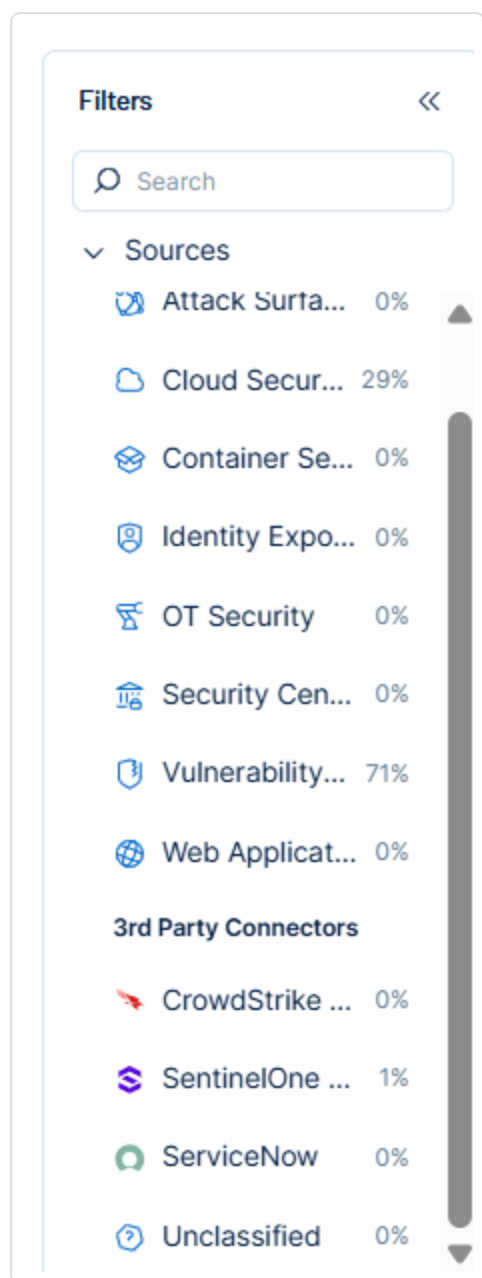
## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Device Mapping

**Tenable**  
**Exposure**      **Qualys Field**  
**Management UI**



Field	
Unique Identifier	<code>id</code>
Asset - External Identifier or Asset - Provider Identifier	<code>CLOUD_RESOURCE_ID</code>
Asset - Name	<code>data.name</code> or <code>DNS</code> or <code>METADATA.VALUE</code> or <code>NAME</code> for 'hostname'
Asset - Operating Systems	<code>OS</code> or <code>data.os</code>
Asset - IPv4 Addresses Asset - IPv6 Addresses	<code>IP</code>
Asset - MAC Addresses	<code>data.networkInterface.list.HostAssetInterface.[*].mac_address</code>
Asset - First Observation Date	<code>data.created</code> or <code>FIRST_FOUND_DATE</code>
Asset - Last Observed At	<code>LAST_VM_SCANNED_DATE</code> or <code>data.lastVulnScan</code>
Asset - External Tags	<code>TAGS</code> <code>METADATA</code> <code>CLOUD_PROVIDER_TAGS</code>
Asset Custom	<code>Host ID</code>



Attributes	Cloud Resource ID
	Hostname
	qualys_id
	Account ID
	Region
	Instance ID
	Image ID
	Instance State
	Tracking Method
	QG Host ID
	Last VM Scanned Date
	Last VM Auth Scanned Date

## Finding Mapping

Tenable Exposure Management UI Field	Qualys Field
Unique Identifier	Host ID + QID + UNIQUE_VULN_ID
Finding Name	data.TITLE
CVEs	data.CVE_LIST.CVE
Severity Driver	data.CVSS_V3.BASE
Description	data.DIAGNOSIS
Finding Custom Attributes	RESULTS.Package.Installed Version data.openPort.list.HostAssetOpenPort
First Seen	FIRST_FOUND_DATETIME
Last seen (Observed)	LAST_FOUND_DATETIME



## Finding Status Mapping

Tenable Exposure Management Status	Qualys Status
Active	All other statuses
Fixed	Fixed Ignored Disabled

**Note:**For Qualys, Exposure Management uses the `report_item_status` field for.

## Finding Severity Mapping

Tenable Exposure Management Severity	Qualys Score
Critical	<b>CVSS:</b> 9.0 - 10.0
High	<b>CVSS:</b> 7.0 - 8.9
Medium	<b>CVSS:</b> 4.0 - 6.9
Low	<b>CVSS:</b> 1-3.9
None	<b>CVSS:</b> 0

**Note:**For Qualys, Tenable uses the `cvss3/cvss` score field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
------------------------------------	-------------------



Archiving Assets	<ul style="list-style-type: none"><li>• Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>• Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a>.</li><li>• Asset that returns from the connector with the state "TERMINATED" (configurable in <a href="#">Data Pulling Configuration</a>).</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>• Finding no longer appears in the scan findings</li><li>• Finding status changes to <code>resolved</code>, <code>ignored</code>, or <code>disabled</code> on the vendor's side.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	<code>id</code>
Finding	<code>ID + QID + UNIQUE_VULN_ID</code>

## API Endpoints in Use

List Hosts version: 4.0

List Agents version: 2.0

Asset Groups version: 3.0

Host List Detection version: 3.0



API	Use in Tenable Exposure Management	Requested Permissions
qualysapi.{{ server_url_postfix }}/api/4.0/fo/asset/host	Fetch Devices - Assets	<p><b>Managers</b> view all scanned hosts within the subscription.</p> <p><b>Auditors</b> view all scanned compliance hosts within the subscription.</p> <p><b>Unit Managers</b> view scanned hosts assigned to the user's business unit.</p> <p><b>Scanners and Readers</b> view scanned hosts assigned to the user's account.</p> <div><p><b>Note:</b> This API returns host information based on the user's role and assigned asset groups in VM/VMDR and PC modules. Access is restricted according to role-based permissions. For Unit Managers, Scanners, and Readers to view compliance hosts, the <b>Manage Compliance</b> permission must be enabled in the user's account settings.</p></div>
qualysapi.{{ server_url_postfix }}/qps/rest/2.0/search/am/hostasset	Devices enrichment	<p><b>Managers</b> with full scope can access the API without additional permissions.</p> <p><b>All other users</b> must have the following permissions</p>



		<p>assigned:</p> <ul style="list-style-type: none"><li>• Access Permission: <b>API Access</b></li><li>• Asset Management Permission: <b>Read Asset</b></li></ul>
<code>qualysapi.{{ server_url_postfix }} /api/3.0/fo/asset/group</code>	Devices enrichment	<p><b>Managers</b> view all asset groups in the subscription.</p> <p><b>Unit Managers</b> view asset groups assigned to their business unit, including groups owned by any user within that unit.</p> <p><b>Scanners and Readers</b> view asset groups assigned to their account, including those they own.</p>
<code>qualysapi.{{ server_url_postfix }} /api/3.0/fo/asset/host/vm/detection</code>	Fetch Detections - Findings	<p><b>Managers</b> view all VM scanned hosts in the subscription.</p> <p><b>Auditors</b> do not have permission to view VM scanned hosts.</p> <p><b>Unit Managers</b> view VM scanned hosts assigned to their business unit.</p> <p><b>Scanners and Readers</b> view VM scanned hosts assigned to their account.</p>



		<b>Note:</b> This API only returns information for hosts assigned to each user through asset groups in VM/VMDR.
<code>qualysapi.{{ server_url_postfix }} /api/3.0/fo/knowledge_base/vuln</code>	Fetch Solutions Detections enrichment	Your subscription must include permission to run this API function.  <b>Auditors</b> do not have permission to download vulnerability data from the Knowledge Base.

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### API Rate Limits and Concurrency

Service Level	Concurrency Limit	Rate Limit
Express/Consultant API Service	1 call	50 calls per day ( <i>not available for Enterprise account</i> )
Standard API Service	2 calls	300 calls per hour
Enterprise API Service	5 calls	750 calls per hour
Premium API Service	10 calls	2000 calls per hour

**Important!** These limits apply per API and per subscription. If multiple connectors use the same subscription, the combined API calls may exceed the allowed limits.





## Subscription Type Selection

The selected **Subscription Type** in the connector configuration directly affects sync behavior and performance.

- **Lower-than-actual subscription tier:** The sync may still succeed, but performance can degrade significantly. Extended sync times may lead to timeouts and eventual sync failure.
- **Higher-than-actual subscription tier:** This can result in API permission errors and cause the sync to fail immediately.

To ensure optimal performance and a successful sync:

- Confirm the correct subscription tier is selected in the connector configuration.
- If multiple connectors share the same subscription, consider staggering their sync schedules to avoid API contention.
- You may lower the configured subscription tier in Vulcan to throttle the sync rate in environments with shared API usage.

## TruRisk (QDS) Scoring Requirements

To use TruRisk (Qualys Detection Score - QDS) within the Exposure Management integration, you must have VMDR (Vulnerability Management, Detection, and Response) enabled on your Qualys subscription.

If the subscription includes only VM (Vulnerability Management) without VMDR, TruRisk scoring will not be available.

### Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Qualys platform.

#### Asset Data Validation

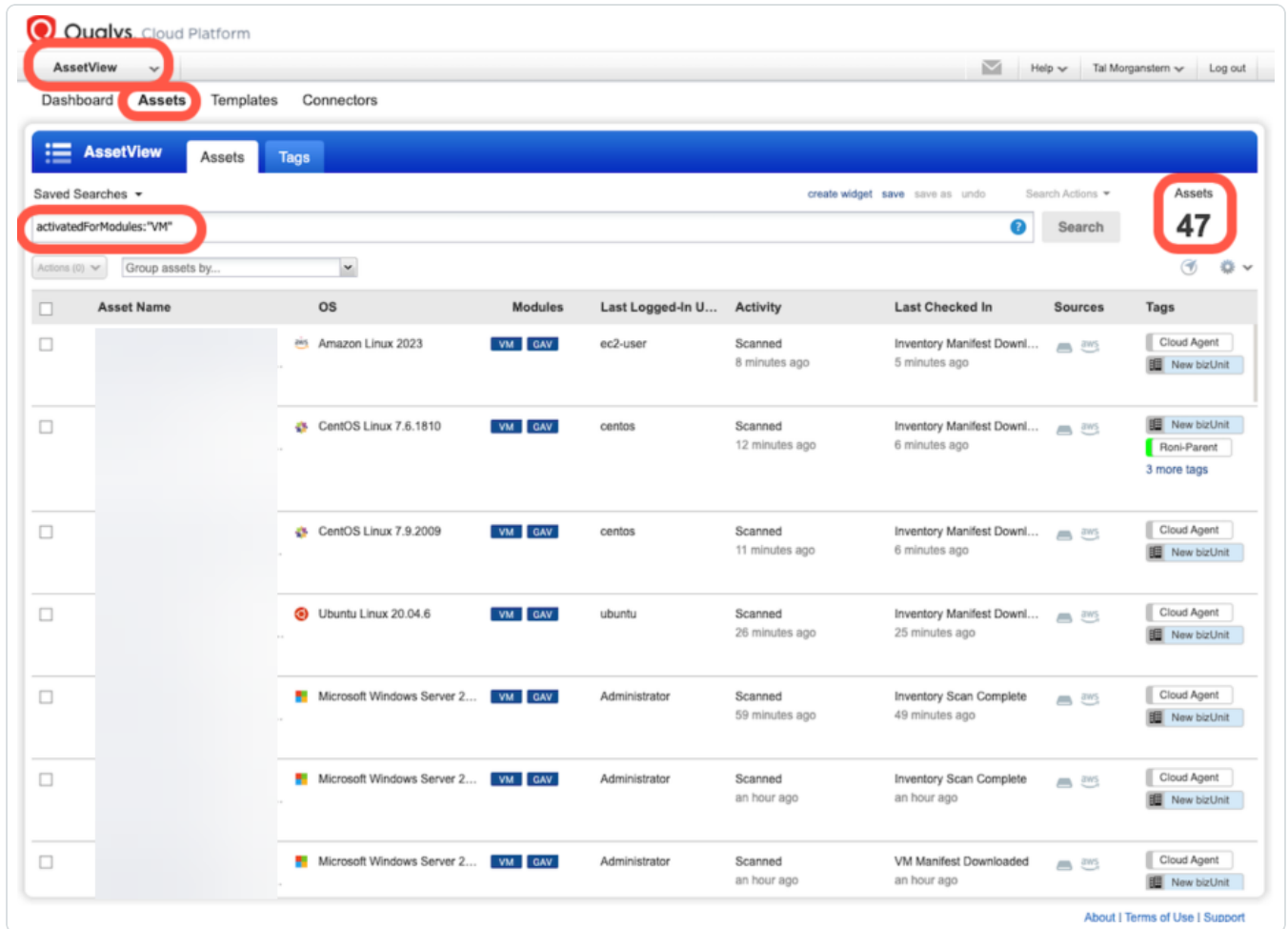
**Objective:** Ensure the number of endpoints (devices) in Qualys aligns with the number of devices displayed in Tenable Exposure Management.

In Qualys:



The Qualys UI does not provide a direct filter to view all assets returned by the hosts endpoint. However, you can validate a subset of these assets through the UI:

1. In the **Asset View** tab, navigate to **Assets**, then search using the filter **activatedForModules:"VM"**.
2. In this example, the filtered view in Qualys shows 47 assets.



In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Qualys and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Qualys and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:



- The asset was archived based on its last observed date (`last_seen` field).
- Asset that returns from the Qualys connector with the state "TERMINATED" (This is the default, but configurable by the user) is archived.
- The asset was archived because it did not return in the connector's last sync.

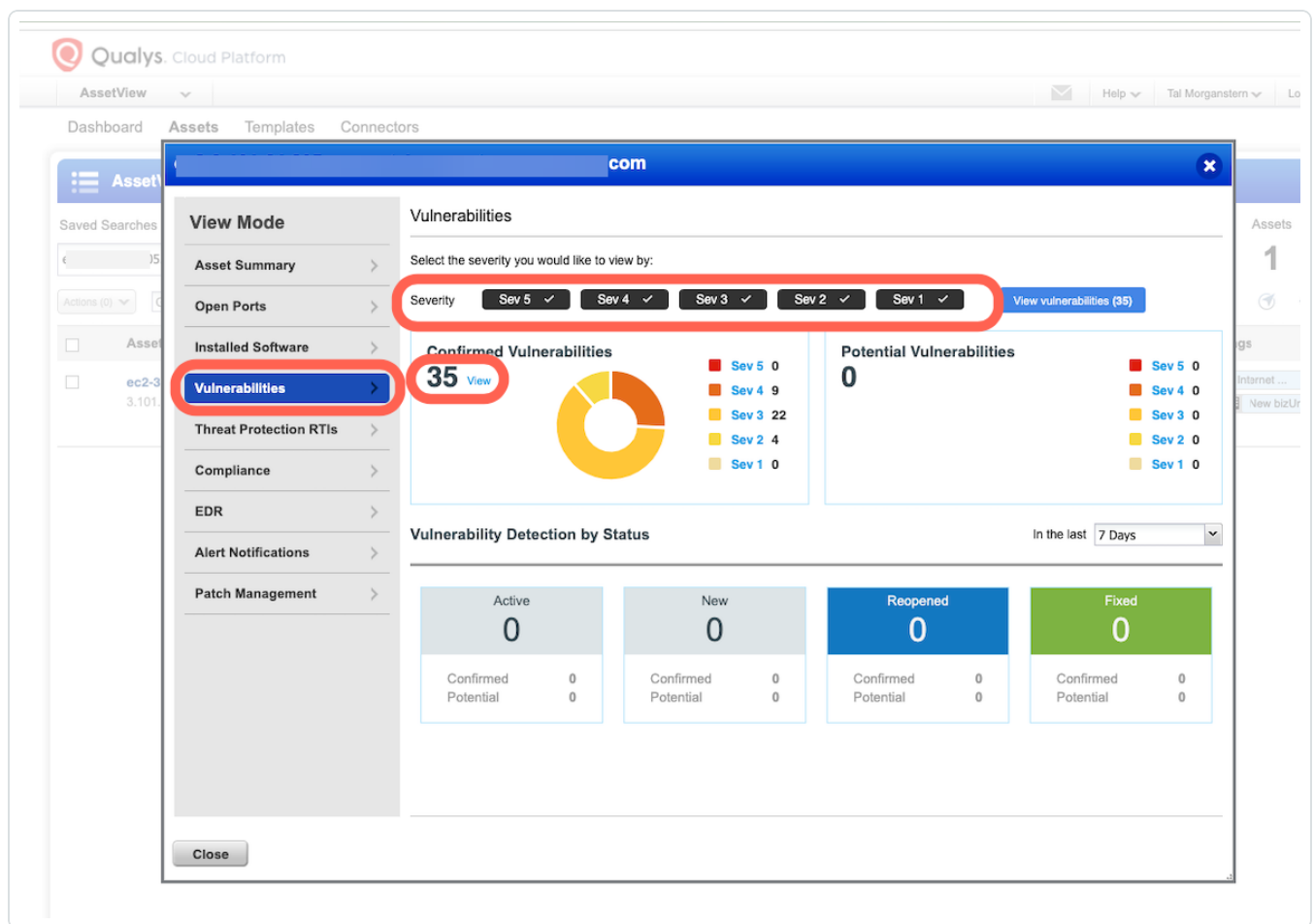
**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## Findings Data Validation

**Objective:** Ensure the number of findings in Qualys aligns with the number of findings in Tenable Exposure Management.

In Qualys:

1. Navigate to the **Assets** view.
2. Click on the asset you want to validate.
3. Navigate to the **Vulnerabilities** tab.
4. Ensure all severities are selected in the filter options.



**Tip:** Only vulnerabilities that are active and not superseded are synced. Apply filters to exclude information, fixed, disabled, and ignored vulnerabilities (if applicable). For accurate comparison, make sure filters in both platforms align by severity, status, and time of sync.

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings in Tenable Exposure Management to the number from CrowdStrike.

**Expected outcome:** The total numbers returned in Qualys and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:



- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## Qualys WAS Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Qualys WAS](#) finds and catalogs all web apps in your network, including new and unknown ones, and scales from a handful of apps to thousands. With Qualys WAS, you can tag your applications with your own labels and then use those labels to control reporting and limit access to scan data.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Qualys WAS</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions



Before you begin configuring the connector, make sure you have the following:

- **Identify the region of your Qualys WAS platform:**

Options include: US1, US2, US3, US4, EU1, EU2, IN1, CA1, AE1, UK1, or AU1

- **Create a Qualys API Reader User with API Permissions:**

Your Qualys subscription must be granted permission to run the API function.

1. In Qualys WAS, navigate to **Administration > User Management**
2. Create a **Reader User**.
3. Fill in the **General** and **Locale** information as required.
4. In the **User Role** section, assign the **Reader Role** with **API** access.

qualysguard.qg2.apps.qualys.eu/fo/options/user\_ae.php?edit=0&user\_role=70#

### New Reader User Launch Help

Users must be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Qualys Integration Partner Service Agreement.

**General Information** >  
**Locale** >  
**User Role** >  
**Asset Groups** >  
**Permissions** >  
**Options** >  
**Security** >

**User Role**  
User Role: \* Reader  
Allow access to: ☐ GUI ☒ API  
Business Unit: \* Unassigned  
New Business Unit

5. In the **Asset Groups** section, select the relevant asset groups you want Tenable Exposure Management to ingest. Only assets from the selected asset groups are ingested into Tenable Exposure Management.
6. In the **Permissions** section, grant the following permissions:

- Manage VM Module
- Manage Web Applications

The screenshot shows a web browser window with the URL `qualysguard.qg2.apps.qualys.eu/fo/options/user_ae.php#`. The page title is "New Reader User" with a "Launch Help" link. A yellow error banner at the top states: "Error! User must be given permission to at least one module. Select 'Manage VM module' and/or 'Manage PC module' in the Permissions section." Below the error, a note reads: "Users must be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Qualys Integration Partner Service Agreement." The left sidebar contains a menu with "Permissions" selected. The main content area, titled "Extended Permissions", lists actions with checkboxes: "Manage VM module" (checked), "Purge host information/history" (unchecked), "Manage PC module" (unchecked), "Manage web applications" (checked), and "Create web applications" (unchecked).

7. For Security, make sure the authentication **is disabled**. If the authentication is enabled, the integration *will not* work.
8. Once the user is saved, edit the user. Under **Roles And Scopes**, Add **WAS User** role to the user **API access** to the **Web Application Scanning** module and Save the user.









The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. From the **Platform** drop-down menu, select the platform on which your Qualys WAS application resides.
4. In the **Username** and **Password** text boxes, paste the credentials for your Qualys WAS account.
5. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.
  - In the **Informational Severity Findings** section:
    - If you want to ingest informational findings from Qualys WAS, select the **Pull informational findings from Qualys WAS** check box.
    - If you want to ingest data from Qualys Knowledge Base, select the **Pull data from Qualys Knowledge Base** check box.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).



6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

❌ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✅ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Qualys WAS in Tenable Exposure Management

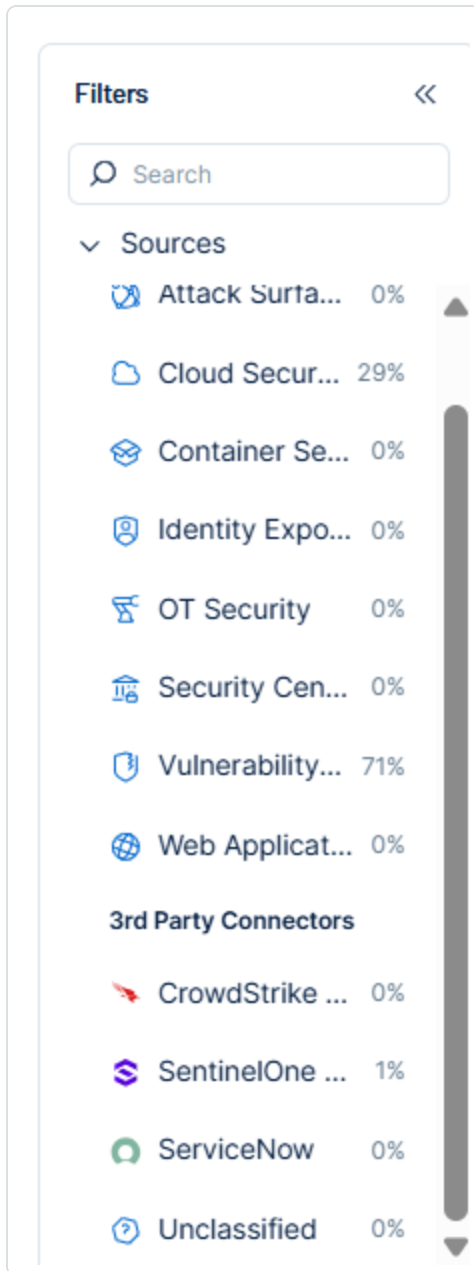
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

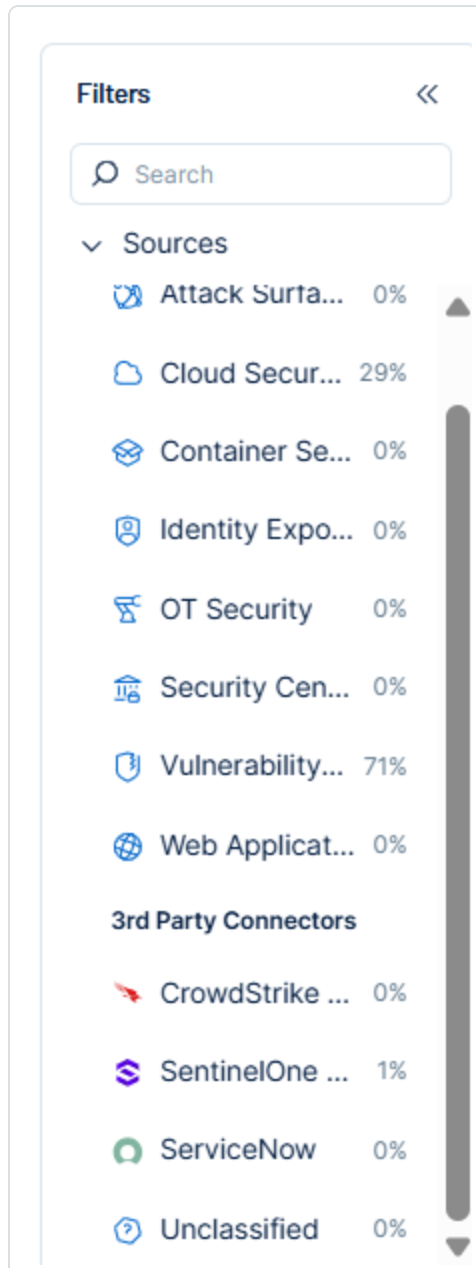
## Locate Connector Weaknesses in Tenable Exposure Management



As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:

1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.





The weaknesses list updates to show only weaknesses from the selected connector.

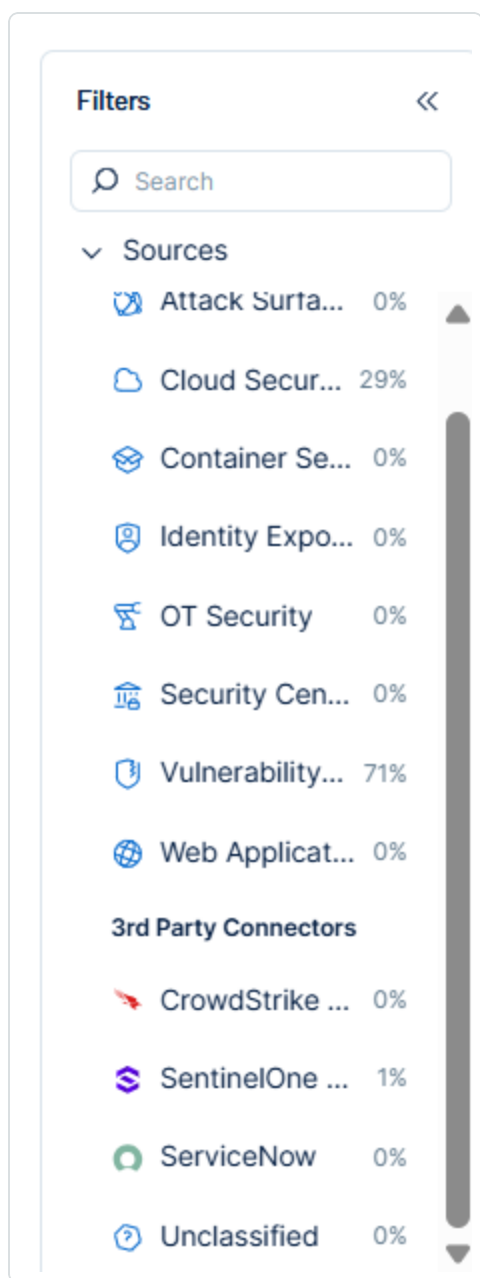
3. Click on any weakness to view [Weakness Details](#).

## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings



The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping



Tenable Exposure Management Value	Qualys WAS Field
Unique Identifier	Webapp.id
Asset - Name	Name
Asset - First Observation Date	Created date
Asset - Last Observed At	Updated date
Asset - Webapp Homepage Screenshot Url	Address
Asset - External Tags	Tags
Asset Custom Attributes	site id site name updated date

## Finding Mapping

Tenable Exposure Management UI Field	Qualys WAS Field
Unique Identifier	Finding.url
Finding Name	Finding.name
CWEs	Finding.cwe.list
Severity Driver	Finding.cvssV3.base
Description	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.DIAGNOSIS
First Seen	Finding.history.set [0].WebAppFindingHistory.scanData.launchDate
Last seen (Observed)	Finding.lastTestedDate
Finding Custom Attributes	Qualys ID Published date





	type
	Impact
	severity
	CVSS V3
	CVSS V3 Temporal
	Attack Vector
	description
	OWASP
	WASC

### Finding Status Mapping

Tenable Exposure Management Status	Qualys WAS Status
Active	new
	active
	reopened
	retesting
	risk accepted
	false positive
	not applicable
Fixed	protected
	fixed

### Finding Severity Mapping

Tenable Exposure Management Severity	Qualys WAS Score
Critical	CVSS: 9.0 - 10.0



High	<b>CVSS: 7.0 - 8.9</b>
Medium	<b>CVSS: 4.0 - 6.9</b>
Low	<b>CVSS: 1-3.9</b>
None	<b>CVSS:0</b>

**Note:**For Qualys WAS, Tenable uses the `Finding.cvssV3.base` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <code>protected</code> or <code>fixed</code> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## API Endpoints in Use

API Version: v3.0

<code>api/2.0/fo/knowledge_base/vuln/</code>	Solutions

## Data Validation



This section shows how to validate and compare data between Tenable Exposure Management and the Qualys WAS platform.

## Asset Data Validation

**Objective:** Ensure the number of Web Applications in Qualys WAS aligns with the number of assets displayed in Tenable Exposure Management.

In Qualys WAS:

1. Navigate to **Web Applications** to see all assets.

Name	# Pages	# Vulns	Severity	MDS Severity	Scanned	Updated
WebGnat.DAST http	0	10	HIGH	N/A	15 Mar 2023	15 Mar 2023
log http	0	1	HIGH	N/A	15 Mar 2023	15 Mar 2023
wak http	0	–	–	N/A	15 Mar 2023	15 Mar 2023
Wa http	0	–	–	N/A	15 Mar 2023	15 Mar 2023
liror http	0	–	–	N/A	15 Mar 2023	15 Mar 2023

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Qualys WAS and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Qualys WAS and Exposure Management should match.



If an asset is not visible in Exposure Management, check the following conditions:

- Archived based on the last observed date (last seen).

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure that the total number of findings between Qualys WAS and Exposure Management is consistent.

In Qualys WAS:

1. Navigate to **Detections** > **Detection List**.
2. On the left filter menu, filter by the relevant web application.

Example:

The screenshot shows the Qualys Enterprise interface. The top navigation bar includes 'Web Application Scanning', 'Dashboard', 'Web Applications', 'Scans', 'Detections', 'Reports', 'Configuration', and 'KnowledgeBase'. The 'Detections' tab is selected, and the 'Detection List' sub-tab is active. On the left, the 'Filter Results' sidebar is open, and the 'Web Application' filter is set to 'LOG4shell'. The main table displays a list of findings with columns for Status, QID, Name, Group, Last Detected, Age, Patch, and Severity. The first finding is a 'New' status finding with QID 150440, named 'Ap...', and a severity of 'INFO'. Below it are several 'DIAG' status findings with QIDs 150152, 45038, 150009, 150020, and 150021. The table also shows a 'Switch to new WAS view!' button in the top right corner.

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
New	150440	Ap...	INFO	16 Dec 2021	502		INFO
-	6	DN	DIAG	16 Dec 2021	502		DIAG
-	6	DN	DIAG	16 Dec 2021	502		DIAG
-	150152	For	DIAG	16 Dec 2021	502		DIAG
-	45038	Ho	DIAG	16 Dec 2021	502		DIAG
-	150009	Lin	DIAG	16 Dec 2021	502		DIAG
-	150020	Lin	DIAG	16 Dec 2021	502		DIAG
-	150021	Sci	DIAG	16 Dec 2021	502		DIAG

3. Note the vulnerability status, as some may be fixed or protected. Filter them out to see only active findings.

In Tenable Exposure Management:



1. [Locate your connector findings.](#)
2. Compare the total number of findings between Qualys WAS and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Qualys WAS and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## Rapid7 Insight AppSec Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Rapid7 Insight AppSec](#) performs black-box security testing to automate identification, triage vulnerabilities, prioritize actions, and remediate application risk.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Rapid7 Insight AppSec</a>
Category	DAST
Ingested data	Assets and Findings



Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Create or use a Rapid7 Insight AppSec user with **Admin** permissions.
- Identify your server URL (e.g., `https://YOURREGION.api.insight.rapid7.com/ias/v1`)
- **Generate a Rapid7 Insight AppSec API Key :**
  1. Navigate to **Settings > API Key > User Key**.
  2. Click **+New User Key**.
  3. Fill in the details
  4. Generate the API Key.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

DAST

Connect

Acunetix Premium

DAST

Connect

Aqua CWPP

CWPP

Connect

Armis

OT

Connect

AWS Config

EDR

Connect

AWS EC2

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

- 707 -



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the Server URL text box, type the server URL for your Rapid7 application.
4. In the **API Key** text box, paste the secret credentials you generated in Rapid7.
5. **Data pulling configuration:** This configuration has dynamic settings tailored to the specific connector and integration type. Below are the configurations relevant to this connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.





Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

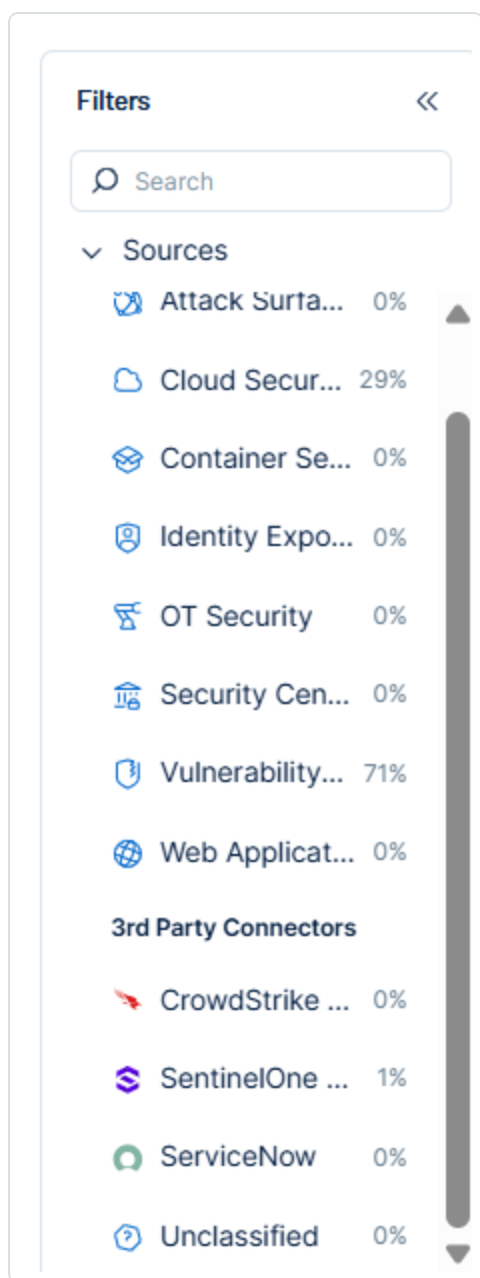
## Rapid7 Insight AppSec in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

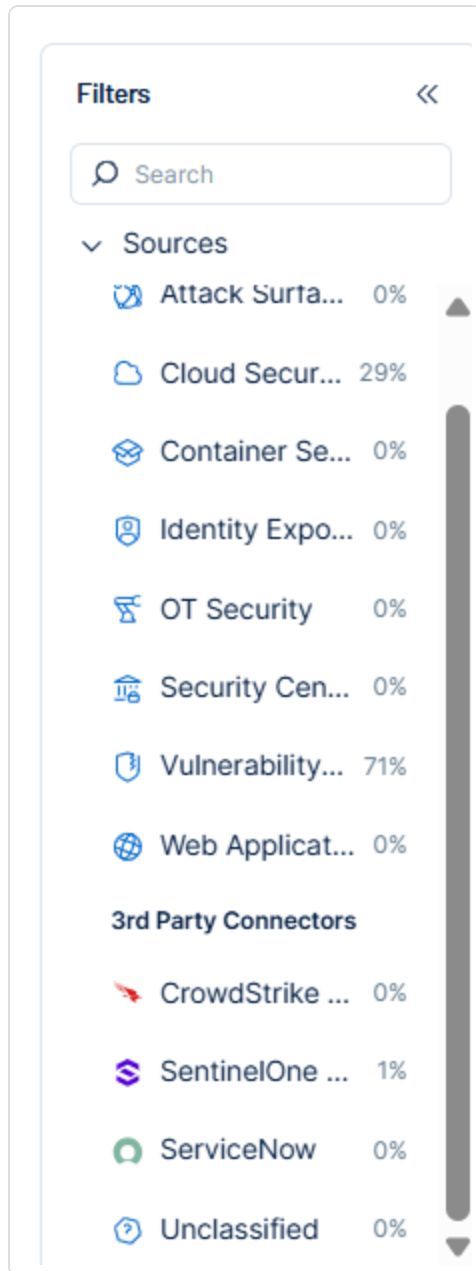
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

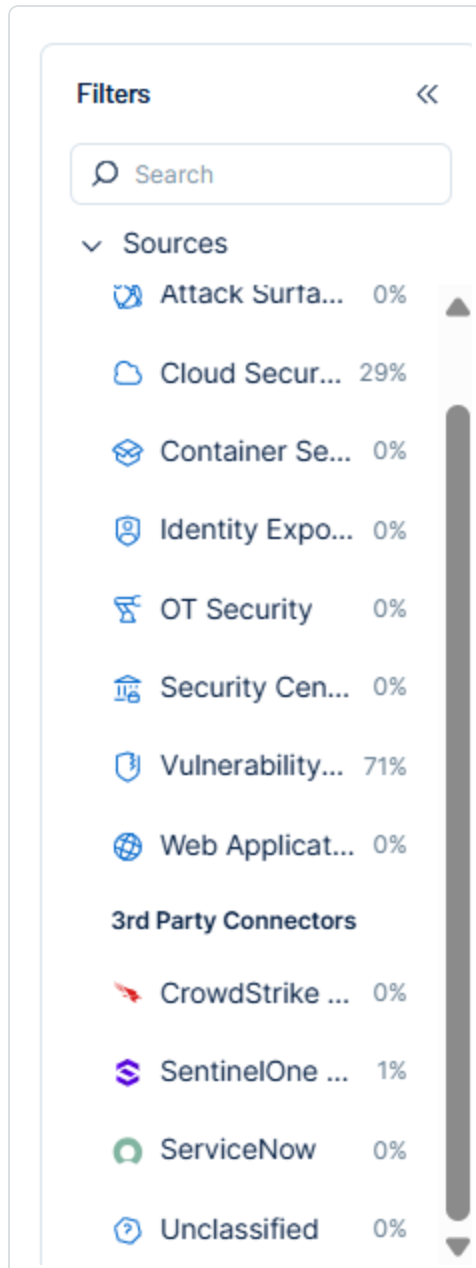
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

### Web Application Mapping

Tenable Exposure Management Value	Rapid7 Insight Appsec Value
Unique Identifier	url_parent
Asset - Name	root_cause.url
Asset - First Observation Date	first_discovered
Asset - Last Observed At	last_discovered
Asset - Webapp Homepage Screenshot Url	root_cause.url
Asset Custom Attributes	app description rapid7 app ID

### Finding Mapping

Tenable Exposure Management UI Field	Rapid7 Insight AppSec Field
Unique Identifier	-
Finding Name	data.name
Severity Driver	cve.base_score or vulnerability_score
Description	data.description
First Seen	first_discovered
Last seen (Observed)	last_discovered



Finding Custom Attributes	<code>module id</code> <code>detailed description</code>  <code>references</code>  <code>CVSS3 vector</code>  <code>rapid7 severity</code>  <code>root cause method</code>  <code>root cause parameter</code>
---------------------------	--

## Finding Status Mapping

Tenable Exposure Management Status	Rapid7 Insight AppSec Status
Active	<code>suppression_info.is_suppressed = TRUE</code>  or  <code>status = expired, open, reopen</code>
Fixed	<code>status = Closed</code>

**Note:**For Rapi7 Insight Appsec, Exposure Management relies mostly on the `status` field to determine finding status. The `suppression_info.is_suppressed` field from the connector is also used in some cases.

## Finding Severity Mapping

Tenable Exposure Management Severity	Rapid7 Insight AppSec Score
Critical	<b>CVSS:</b> 9-10  <b>Severity:</b> Critical
High	<b>CVSS:</b> 7-8



	<b>Severity:</b> High
Medium	<b>CVSS:</b> 4-6 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:** For Rapid7 Insight Appsec, Exposure Management uses the `cve.base_score` field to determine severity. If `cve.base_score` not available, Exposure Management uses the `ulnulnerabilitySeverityLevel` field from the connector, if provided.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria



Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	url_parent

### API Endpoints in Use

API	Use in Tenable Exposure Management
{{ server_url }}/vulnerabilities	Findings
{{ server_url }}/modules	Findings enrichment
{{ server_url }}/apps	Assets

## Rapid7 Insight VM (On-Prem) Connector

[Rapid7](#) InsightVM solution discovers risks across all your endpoints, cloud, and virtualized infrastructure. Tenable Exposure Management integrates with Rapid7 InsightVM to ingest assets and their associated vulnerabilities from your on-premises environment. This connector is based on scheduled reports and requires you to create dedicated report templates within the Rapid7 console. During each sync, the connector retrieves vulnerability and asset data from these reports to provide visibility into risks across your endpoints, virtual machines, and infrastructure. The integration helps you prioritize vulnerabilities, track remediation efforts, and monitor your security posture directly within Exposure Management.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details





Details	Description
Supported products	<a href="#">Rapid7 Insight VM (On-Prem)</a> <div><b>Important!</b> This guide describes the <a href="#">InsightVM Application Programming Interface (API) version 3</a>. The API follows the Representational State Transfer (REST) design pattern and, unless stated otherwise, uses JSON (application/json) as the default request and response format. The API is hypermedia-friendly and implements Hypermedia as the Engine of Application State (HATEOAS) principles. All API requests must be made over HTTPS to the Security Console.</div>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Identify your Rapid7 Server URL (e.g., `https://<your-server-hostname>:<port>`).
- Review the [System Requirements](#) for your deployment environment.

**Important!** The performance of the connector, including synchronization times, depends on the system configuration of the Rapid7 Security Console. Ensure that your environment meets the system requirements to avoid degraded performance or sync failures.

- **Create a Rapid7 user with the appropriate permissions:**

To create a Rapid7 user with the appropriate permissions:



1. Sign in to the Rapid7 console using a **Global Admin** account.
2. Navigate to **Administration**.
3. In the **Users** section, click **Create**.
4. In the General section, enter the required user details and select the **Account enabled** checkbox.

For example:

The screenshot shows the 'Create User' form in the Rapid7 console, specifically the 'GENERAL' section. On the left is a dark sidebar with navigation links: 'GENERAL' (selected), 'ROLES', 'SITE ACCESS', and 'ASSET GROUP ACCESS'. The main content area has a header with instructions: 'Enter information that will identify this user. Select an authentication method if more than one is available. Consult your network administrator about multiple authentication options. This access the Security Console unless you select the check box to enable the account. You can clear the check box at any time to take away access.' Below this are several input fields: 'User name' (vulcan-user), 'Authentication method' (InsightVM user), 'Full name' (vulcan), 'E-mail address' (support@vulcan.io), 'Password' (masked with dots), and 'Confirm password' (masked with dots). At the bottom are two checkboxes: 'Account enabled' (checked) and 'Require password reset upon login' (unchecked).

5. In the **Roles** section, select the **User** role. Then, for Global Permissions, select the **Appear on Ticket and Report Lists** checkbox.
6. In the **Site Access** section, select the **Allow this user to access all sites** option.
7. In the **Asset Group Access** section, select the **Allow this user to access all asset groups** option.
8. Click **Save** to create the user.

Save the username and password in a secure location. You will need these credentials later when you configure the connector in the Exposure Management platform.

#### • Create Rapid7 Report Templates:



To set up the Rapid7 InsightVM integration, you *must* create the following three report templates:

## Assets Report Template

To create an asset report template:

1. In Rapid7, navigate to **Create > Report**.
2. Click **Manage Report Templates > New**.
3. Name the template: `tenable_assets_report_template`

**Important:** This name must match exactly, or the connector configuration will fail.

4. (Optional) Type a description.
5. In the **Template Type** section, select **Export (CSV format)**.
6. In the **Content** section, select the following fields:
  - Asset Alternate IPv4 Addresses,
  - Asset Alternate IPv6 Addresses
  - Asset ID
  - Asset IP Address
  - Asset Names
  - Asset OS Family
  - Asset OS Name
  - Asset OS Version
  - Asset Risk Score
  - Custom Tag
  - Asset Location



- Asset Criticality
- Asset MAC Addresses
- Asset Owner
- Site Name
- Site Importance

7. Click **Save**.

The screenshot shows the configuration interface for an 'Assets and Findings Details Report Template'. At the top, there are three input fields: 'Name' (containing 'tenable\_assets\_report\_template'), 'Description' (containing 'Tenable One Integration'), and 'Template type' (a dropdown menu set to 'Export (CSV format)'). Below these fields is a section titled 'Select data fields to include in the template'. It features two columns of fields. The left column contains: Exploit Count, Exploit Minimum Skill, Exploit URLs, Malware Kit Count, Malware Kit Names, Reintroduced Date, Scan ID, Scan Template Name, Service Name, Service Port, Service Product, Service Protocol, Vulnerability Additional URLs, and Vulnerability Age. The right column contains: Asset Alternate IPv4 Addresses, Asset Alternate IPv6 Addresses, Asset IP Address, Asset Names, Asset OS Family, Asset OS Name, Asset OS Version, Asset Risk Score, Custom Tag, Asset Location, Asset Criticality (highlighted in blue), Asset MAC Addresses, and Asset Owner. A tooltip points to the right column with the text 'These are the asset criticality tags.' Between the columns are 'Add >' and '< Remove' buttons. A 'Clear' button is at the bottom right of the field selection area. At the very bottom of the form are 'SAVE' and 'CANCEL' buttons.

## Assets and Findings Details Report Template

To create an assets and findings details report template:



1. In Rapid7, navigate to **Create > Report**.
2. Click **Manage Report Templates > New**.
3. Name the template: `tenable_assets_findings_detailed_report_template`

**Important:** This name must match exactly, or the connector configuration will fail.

4. (Optional) Type a description.
5. In the **Template Type** section, select **Export (CSV format)**.
6. In the **Content** section, select the following fields:

- Asset ID
- Vulnerability ID
- Vulnerability Description
- Vulnerability CVSSv3 Vector
- Vulnerability CVSSv3 Vector
- Vulnerability CVSS Score
- Vulnerability Risk Score
- Vulnerability Solution
- Vulnerability Title
- Vulnerable Since
- Vulnerability Test Date
- Vulnerability CVE IDs
- Vulnerability Age
- Exploit Count
- Service Port



- Service Protocol
- Vulnerability Proof
- Vulnerability Published Date

7. Click **Save**.

Name:

Description:

Template type:

Select data fields to include in the template

Available Fields	Selected Fields
Asset Alternate IPv4 Addresses	Asset ID
Asset Alternate IPv6 Addresses	Vulnerability ID
Asset Criticality	Vulnerability Description
Asset IP Address	Vulnerability CVSSv3 Vector
Asset Location	Vulnerability CVSSv3 Score
Asset MAC Addresses	Vulnerability CVSS Score
Asset Names	Vulnerability Risk Score
Asset OS Family	Vulnerability Solution
Asset OS Name	Vulnerability Title
Asset OS Version	Vulnerable Since
Asset Owner	Vulnerability Test Date
Asset Risk Score	Vulnerability CVE IDs
Custom Tag	Vulnerability Age
Exploit Minimum Skill	Vulnerability Proof

Buttons: Add >, < Remove, Clear

Bottom Bar: SAVE, CANCEL

## Assets and Findings Report Template

To create an assets and findings report template:

1. In Rapid7, navigate to **Create > Report**.
2. Click **Manage Report Templates > New**.
3. Name the template: `tenable_assets_findings_report_template`



**Important:** This name must match exactly, or the connector configuration will fail.

4. (Optional) Type a description.
5. In the **Template Type** section, select **Export (CSV format)**.
6. In the **Content** section, select the following fields:
  - Asset ID
  - Vulnerability ID
  - Vulnerable Since
  - Vulnerability Test Date
  - Vulnerability Proof
  - Service Port
  - Service Protocol
7. Click **Save**.



Name

tenable\_assets\_findings\_report\_template

Description

Tenable One Integration

Template type

Export (CSV format)

Select data fields to include in the template

Asset Alternate IPv4 Addresses

Asset Alternate IPv6 Addresses

Asset Criticality

Asset IP Address

Asset Location

Asset MAC Addresses

Asset Names

Asset OS Family

Asset OS Name

Asset OS Version

Asset Owner

Asset Risk Score

Custom Tag

Exploit Count

Asset ID

Vulnerability ID

Vulnerable Since

Vulnerability Test Date

Vulnerability Proof

Service Port

Service Protocol

Add >

< Remove

Clear

SAVE

CANCEL

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.


















Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

Configure the Rapid7 Insight VM Connector



1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server URL** text box, type the server URL for your Rapid7 instance.
4. In the **Username** and **Password** text boxes, type your Rapid7 client credentials.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.



### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

⊗ Failed tests 1 out of 4 integration tests failed

✓ Successful tests 3 out of 4 integration tests succeeded

[Test connectivity](#)[Show tests](#) [Show tests](#) 



7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

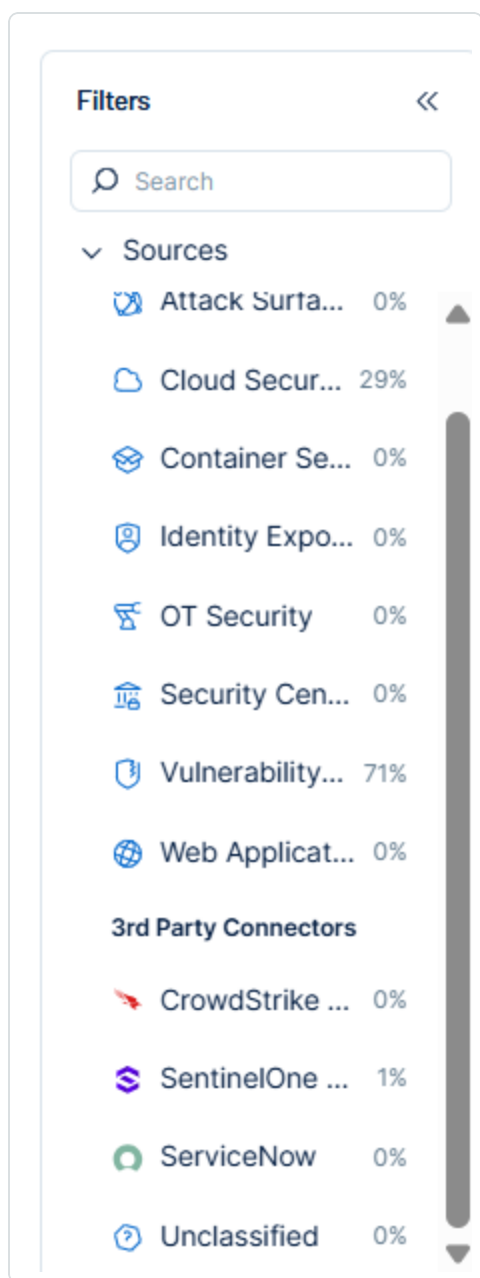
## Rapid7 Insight VM in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

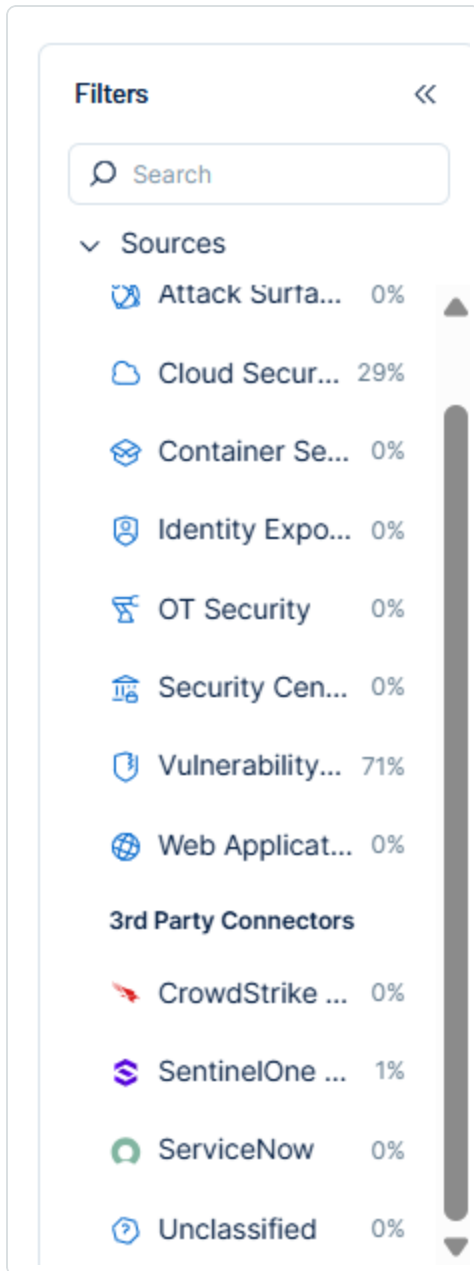
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

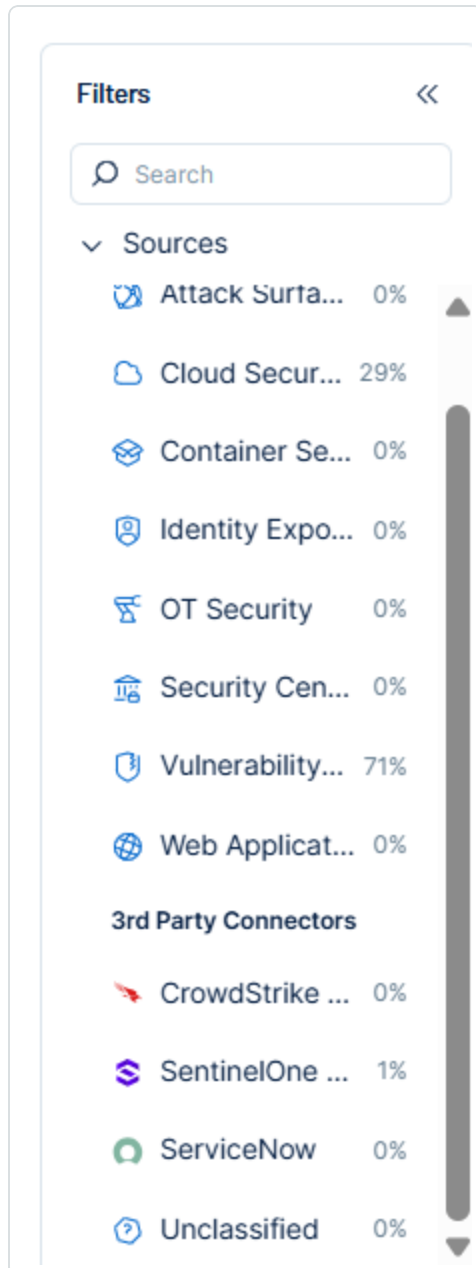
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Rapid7 InsightVM (On-Prem) field
Unique Identifier	id
Asset - Name	hostName or Asset Names <div><b>Note:</b> In rare cases where the hostname is not available, the IP address is used as a fallback.</div>
Asset - Operating Systems	os or osFingerprint.vendor/Asset OS Name
Asset - Host Fully Qualified DNS	host_name
Asset - IPv4 Adresses Asset - IPv6 Adresses	ip or Asset IP Address
Asset - Mac Address	mac or address.mac or Asset MAC AddressesAsset MAC Addresses
Asset - First Observation Date	history[0].date
Asset - Last Observed At	history[-1].date
Asset - Host Fully Qualified DNS	hostName or Asset Names



Asset - External Tags	Custom Tag Site Name Asset Owner Asset Criticality Site Importance Asset Location
Asset Custom Attributes	osFingerprint.os/os Asset OS Family/osFingerprint.family

## Finding Mapping

Tenable Exposure Management UI Field	Rapid7 InsightVM (On-Prem) field
Unique Identifier	Vulnerability ID + Service Protocol + Service Port
Finding Name	Vulnerability Title
CVEs	Vulnerability CVE IDs
Severity Driver	Vulnerability CVSSv3 Score
Description	Vulnerability Description
Finding Custom Attributes	Vulnerability Proof Service Port Service Protocol Vulnerability CVSSv3 Vector
First Seen	Vulnerable Since
Last seen (Observed)	Vulnerability Test Date

## Finding Status Mapping





Tenable Exposure Management Status	Rapid7 InsightVM (On-Prem) Status / Condition
Active	All ingested findings are considered active
Fixed	Findings no longer appear in the scan findings

## Finding Severity Mapping

Tenable Exposure Management Severity	Rapid7 InsightVM (On-Prem) Score
Critical	<b>CVSS v3:</b> 9.0 - 10.0
High	<b>CVSS v3:</b> 7.0 - 8.9
Medium	<b>CVSS v3:</b> 4.0 - 6.9
Low	<b>CVSS v3:</b> 1-3.9
None	<b>CVSS v3:</b> 0

**Note:**For Rapid7 Insight VM On-Prem, Tenable uses the Vulnerability CVSSv3 Score field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	- Asset not seen for X days according to <b>Last Seen</b> . See <a href="#">Asset Retention</a>
Change of a Finding status from "Active" to "Fixed"	- Finding no longer appears in the scan findings



**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Finding	Vulnerability ID + Service Protocol + Service Port
Detection	Vulnerability ID
Solution	Vulnerability Solution

## API Endpoints in Use

**API:** V3

API	Use in Tenable Exposure Management	Required Permissions
GET <code>{{ server_url }}/api/3/sites</code>	-	Allow listing sites
POST <code>{{ server_url }}/api/3/report</code>	-	Allow create report
POST <code>{{ server_url }}/api/3/reports/{{ report_id }}/generate</code>	-	Allow generating



		domains
GET#{{ server_url }}/api/3/reports/{{ report_id }}/history/{{ report_instance_id }}/output	Assets, Findings, Solutions	Allow read report
GET {{ server_url }}/api/3/tags	Asset tags	-
GET #{{ server_url }}/api/3/asset_groups	Asset tags	Allow listing asset_groups
GET server_url }}/api/3/asset_groups/{{ asset_group_id }}/assets	Asset tags	Allow listing asset_groups assets
GET {{ server_url }}/api/3/vulnerabilities	Findings (Only on report_with_api variant)	-

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Report Generation Requirement

The connector generates reports as part of the integration process. To ensure successful synchronization, customers must create report templates as [outlined in this guide](#).

**Important!** The connector cannot function properly without the required report templates.

### System Requirements

The performance of the connector, including synchronization times, depends on the system specifications of the Rapid7 Security Console. Failing to meet the recommended system specifications can result in increased sync durations, performance degradation, or failures in data collection.



Ensure that your environment meets the following requirements to avoid degraded performance or sync failures:

#### General Requirements:

- At this time, Tenable Exposure Management only supports **x86\_64 architecture**.
- If deploying to a virtual machine:
  - Allocate sufficient reserved memory based on system requirements.
  - The reserved memory value must match the allocated memory. For example, if 32 GB is allocated, reserved memory must also be set to 32 GB.
  - Using shared or overcommitted memory may negatively affect performance and can lead to out-of-memory events.

#### Security Console Hardware Requirements:

Asset Volume	Processor	Memory	Storage
5,000	4 Cores	16 GB	1 TB
20,000	12 Cores	64 GB	2 TB
150,000	12 Cores	128 GB	4 TB
400,000	12 Cores	256 GB	8 TB

How can I Check Machine Hardware in the Rapid7 Console?

1. Navigate to **Administration > Troubleshooting > Run Commands**.
2. In the input field, type `show host`, and then click **Execute**.



For example:

Type a command in the box and then click **Execute** to run the command. For list of available commands, type *help* or *?*. For more information see [using the command console](#).

show host

**EXECUTE**

Current directory:	/	nsc
User name:	root	
Super user:	Yes	
Computer name:	i	7
Host Address:	17	17
Host FQDN:	ip	hal
Operating system:	Ubuntu Linux 18.04	
CPU speed:	2199MHz	
Number of CPUs:	4	
Total memory:	15.5 GB	
Available memory:	346.2 MB	
Total disk space:	96.9 GB	
Available disk space:	52.4 GB	
Disk space used by installation:	30.3 GB	
Disk space used by scans:	284.9 MB	
Disk space used by database:	4.8 GB	
Disk space used by reports:	2 KB	
Disk space used by backups:	0 bytes	
JVM name:	0	VM
JVM vendor:	Azul Systems, Inc.	
JVM version:	17.0.13+11-LTS	
JVM started:	2025-04-30 15:53 GMT	

**Note:** For more information, see [Rapid7 On-Prem System Requirements](#).

## Finding Uniqueness Criteria

Findings are considered unique based on the following combination of fields:

- Vulnerability ID
- Service Protocol

The integration *does not* consider the **Proof** field as part of the uniqueness criteria. If multiple proofs exist for the same finding, only one will be displayed in Exposure Management.

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Rapid7 Insight VM On-Prem platform.

## Asset Data Validation



**Objective:** Ensure the number of scanned virtual machines (VMs) in Rapid7 Insight VM On-Prem aligns with the assets (devices) displayed in Tenable Exposure Management.

In Rapid7 Insight VM On-Prem:

1. In the left menu, click **Assets**

The asset table appears.

2. The asset table displays all scanned virtual machines.

The total number of assets will appear on the bottom of the screen.

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between Rapid7 Insight VM On-Prem and Tenable Exposure Management.

**Expected outcome:** The number of visible assets in Exposure Management will match the number of VM assets in Rapid7.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived based on the last observed date (last seen).

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure the number of vulnerabilities associated with assets in Rapid7 InsightVM aligns with the findings displayed in Tenable Exposure Management.

In Rapid7 InsightVM:

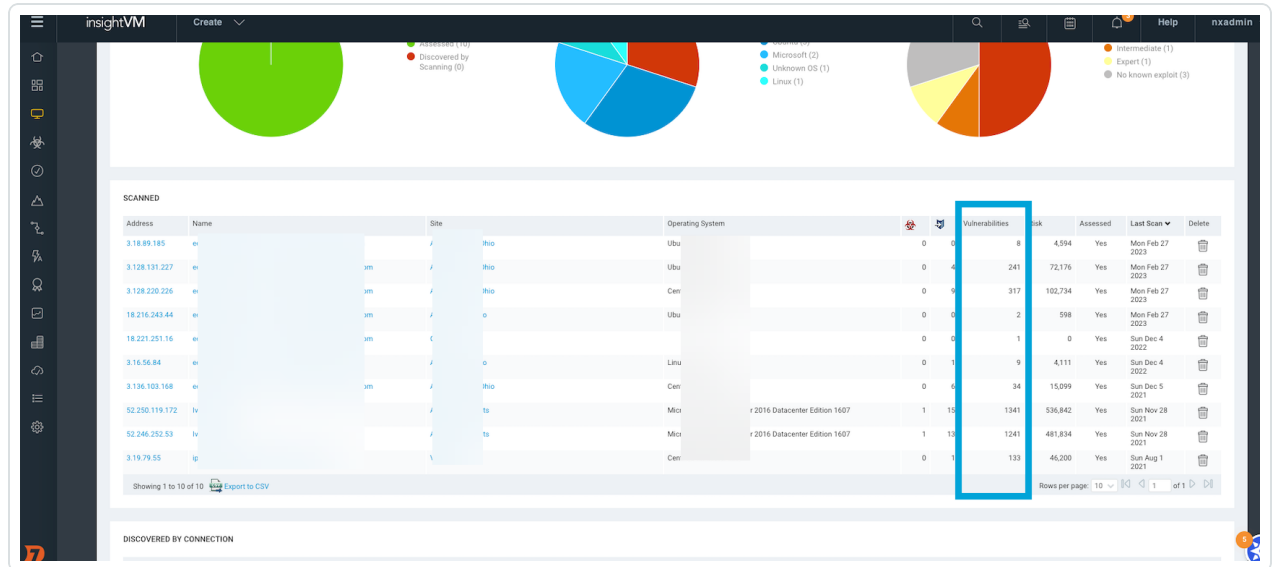
You can view vulnerabilities (findings) in Rapid7 in one of the following ways:



- Through the **Assets** view:

1. Navigate to **Assets**.

In the **Assets** table view, each asset row displays a count of associated vulnerabilities.



2. To get the findings total, sum the total number of vulnerabilities across all assets.

- Through the **Vulnerabilities** view:

1. Navigate to **Vulnerabilities**.
2. Scroll down to view the vulnerabilities table. This table is aggregated by unique

vulnerability name and displays the number of findings for each vulnerability.

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between Rapid7 Insight VM On-Prem and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Rapid7 Insight VM On-Prem and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding no longer appears in the scan findings.
- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).





## Rapid7 InsightVM Cloud Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The [Rapid7](#) InsightVM Cloud solution identifies risks across all endpoints, cloud environments, and virtualized infrastructure. It enables comprehensive network scanning, prioritizes vulnerabilities, and provides actionable remediation guidance for IT and DevOps teams. InsightVM also offers real-time visibility into your risk posture and helps track and communicate progress toward security program goals.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">Rapid7 Insight VM Cloud (Vulnerability Assessment)</a>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Device
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

### Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:



- Identify the region of your Rapid7 InsightVM Cloud instance (United States, Europe, Canada, Australia, or Japan).
- Create or use a Rapid7 InsightVM Cloud user with **Admin** permissions.
- **Generate a Rapid7 API Key:**
  1. Login to Rapid7 using an **Admin** user.
  2. Navigate to **Settings > API Keys**.
  3. Click **GenerateNew User Key**.
  4. Select the appropriate organization, assign a name to the API key, and click **Submit**.



### Generate New User Key

A user API key is associated with a single user and inherits all permissions of that user.

Organization

Select Organization

Name

Submit

Cancel

4



5. Copy the API key immediately, as it will only be visible during its creation. You will use this API key later when configuring the Rapid7 InsightVM Cloud connector in Exposure Management.

## Add a Connector

To add a new connector:
















1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

# Connectors

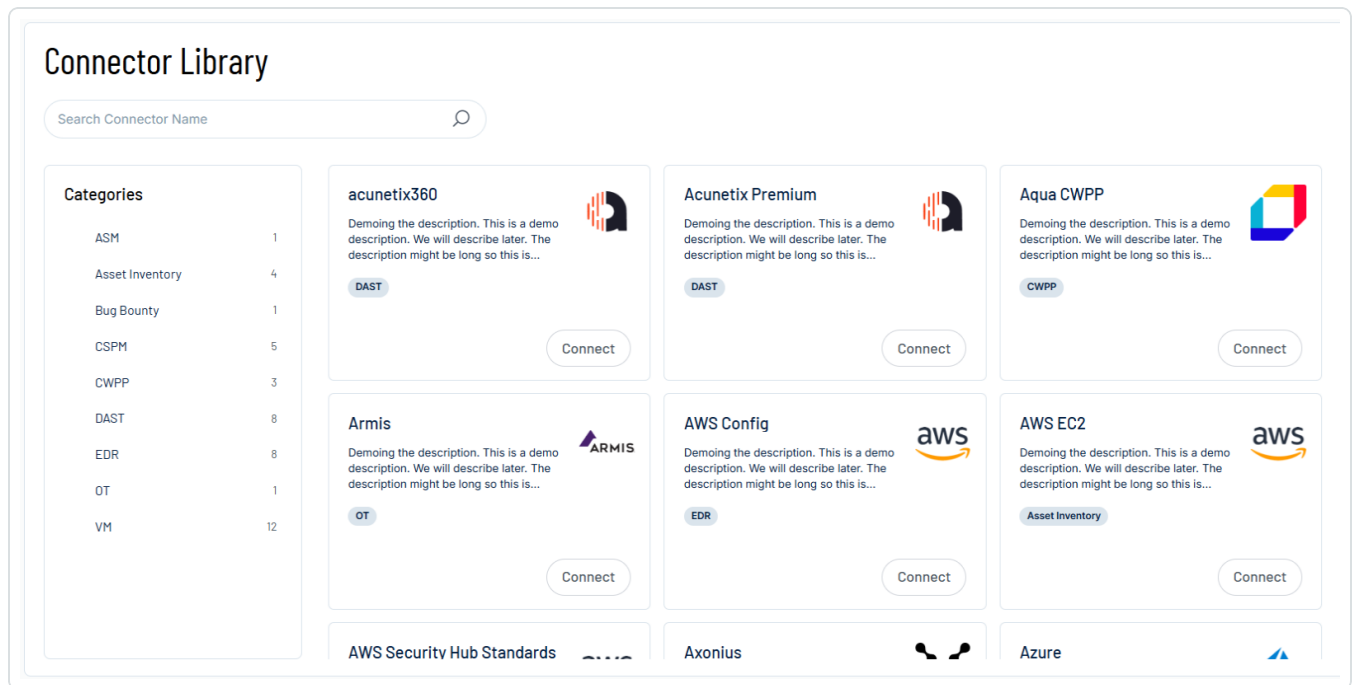
Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	⋮
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	⋮
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	⋮
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	⋮
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	⋮
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	⋮
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	⋮

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Rapid7 Insight VM Cloud Connector

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Region** drop-down, select the relevant region of your Rapid7 instance.
4. In the **API Key** text box, paste the API Key you generated in Rapid7.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.



- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.

- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

Show tests ▼

**Successful tests** 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.

9. To confirm the sync is complete, do the following:

- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.



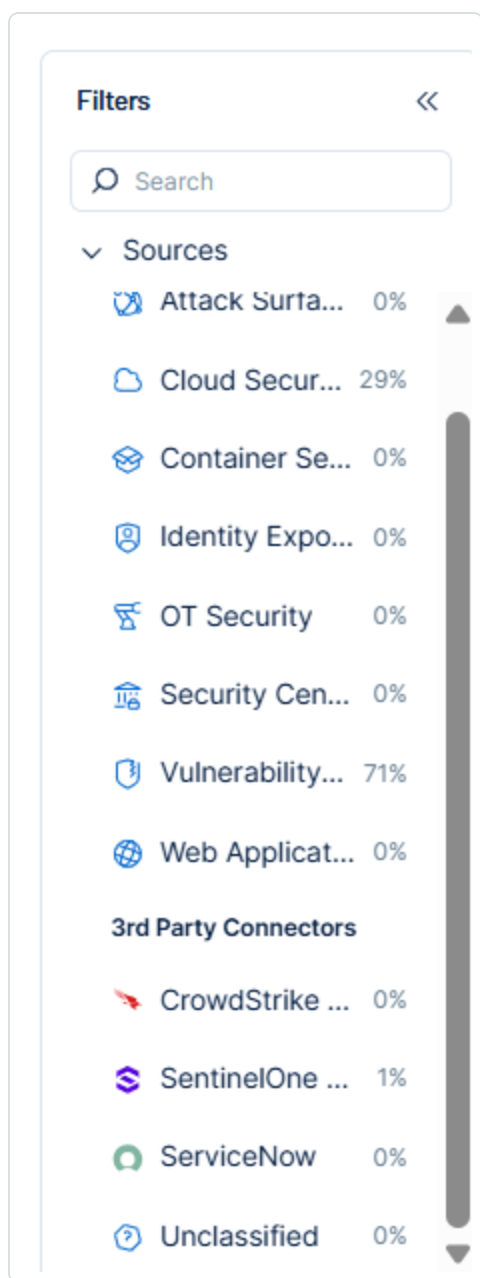
## Rapid7 Insight VM Cloud in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Locate Connector Weaknesses in Tenable Exposure Management

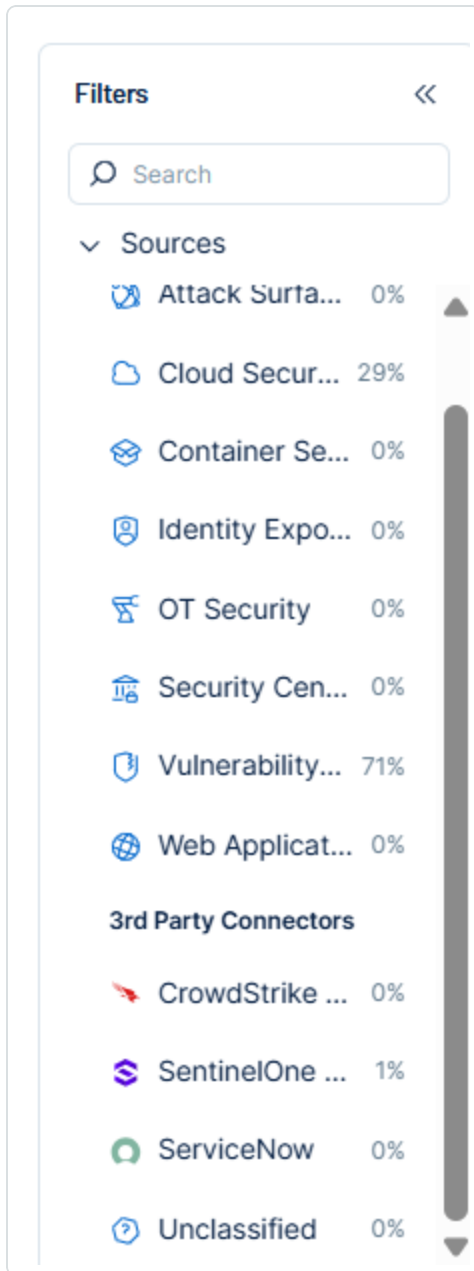
As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:





1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

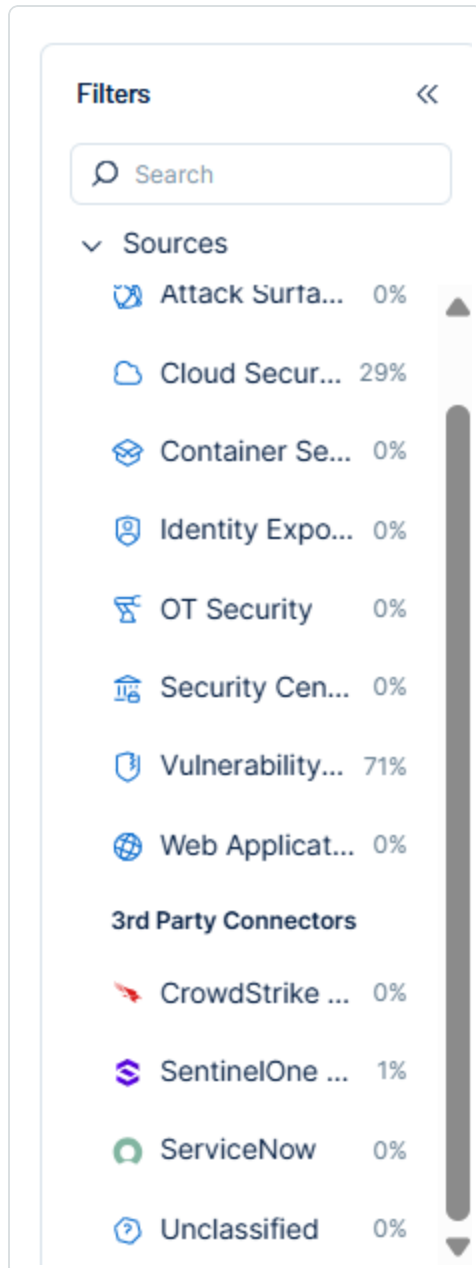
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Rapid7 InsightVM Cloud field
Unique Identifier	id
Asset - Name	host_name or ip or id
Asset - Operating Systems	os_system_name or os_name or os_family
Asset - Host Fully Qualified DNS	host_name
Asset - IPv4 Adresses	ip
Asset - IPv6 Adresses	
Asset - Last Observed At	last_scan_end or last_assessed_for_vulnerabilities
Asset - External Tags	tags.name from tags
Asset Custom Attributes	os_version os_description Host ID- id type os_architecture risk_score

## Finding Mapping



Tenable Exposure Management UI Field	Rapid7 InsightVM Cloud field
Unique Identifier	port and protocol
Finding Name	data.title
CVEs	data.cves
Severity Driver	data.severity_score or data.cvss_v3_score
Description	data.description
Finding Custom Attributes	port protocol proof status data.categories data.cvss_v2_exploit_score data.cvss_v2_impact_score data.cvss_v2_score data.cvss_v2_vector data.cvss_v3_attack_complexity data.cvss_v3_attack_vector data.cvss_v3_availability_impact data.cvss_v3_confidentiality_impact data.cvss_v3_exploit_score data.cvss_v3_impact_score data.denial_of_service data.pci_cvss_score data.pci_fail



	<code>data.pci_severity_score</code> <code>data.pci_special_notes</code> <code>data.pci_status</code> <code>data.references</code> <code>data.risk_score</code> <code>data.severity</code> <code>data.severity_score</code>
First Seen	<code>first_found</code>
Last seen (Observed)	<code>last_found</code>

### Finding Status Mapping

Tenable Exposure Management Status	Rapid7 InsightVM Cloud Status
Active	All other statuses including EXCEPTION_VULN_EXPL or EXCEPTION_VULN_VERS
Fixed	NOT_VULNERABLE

### Finding Severity Mapping

Tenable Exposure Management Severity	Rapid7 InsightVM Cloud Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9



	<b>Severity:</b> Low
None	<b>CVSS:</b> 0

**Note:** For Rapid7 Insight VM Cloud, Tenable uses the `data.severity_score` or `cvssScore` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>- Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync</li><li>- Asset not seen for X days according to <b>Last Seen</b>. See <a href="#">Asset Retention</a>.</li></ul>
Change of a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>- Finding no longer appears in the scan findings</li><li>- Finding status changes to NOT_VULNERABLE on the vendor's side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).



The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Finding	port and protocol

## API Endpoints in Use

API version: v4.0

API	Use in Tenable Exposure Management
vm/v4/integration/vulnerabilities	Findings enrichment
vm/v4/integration/asset	Mapping Assets & Findings

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Rapid7 InsightVM Cloud platform.

### Asset Data Validation

**Objective:** Ensure the number of assets (devices) in Rapid7 InsightVM Cloud aligns with the number of devices displayed in Tenable Exposure Management.

In Rapid7 InsightVM Cloud:

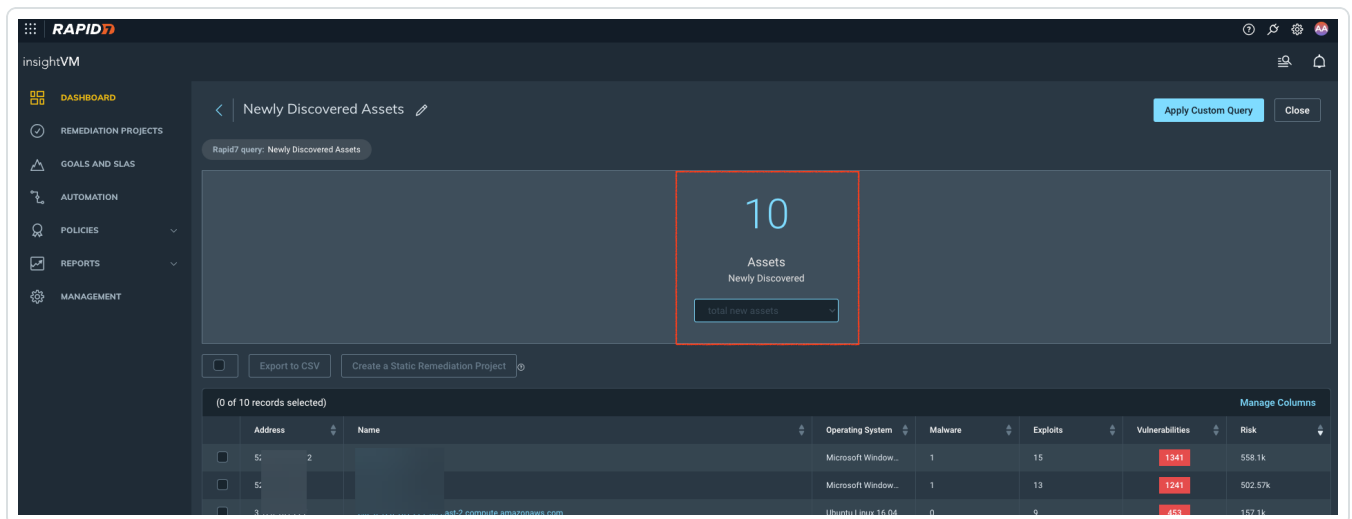


## 1. Navigate to **Dashboard > Newly Discovered Assets**.



## 2. Click **Total new assets**.

The total number of newly discovered assets appears.



In Tenable Exposure Management:





1. [Locate your connector assets.](#)
2. Compare the total number of assets between Rapid7 InsightVM Cloud and Tenable Exposure Management.

**Expected outcome:** The total number of devices in Exposure Management should match the number of assets shown in Rapid7.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on its last observed date (`last_seen` field).
- The asset was archived because it did not return in the connector's last sync.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## Finding Data Validation

**Objective:** Ensure the number of active findings in Rapid7 InsightVM Cloud aligns with the findings displayed in Exposure Management.

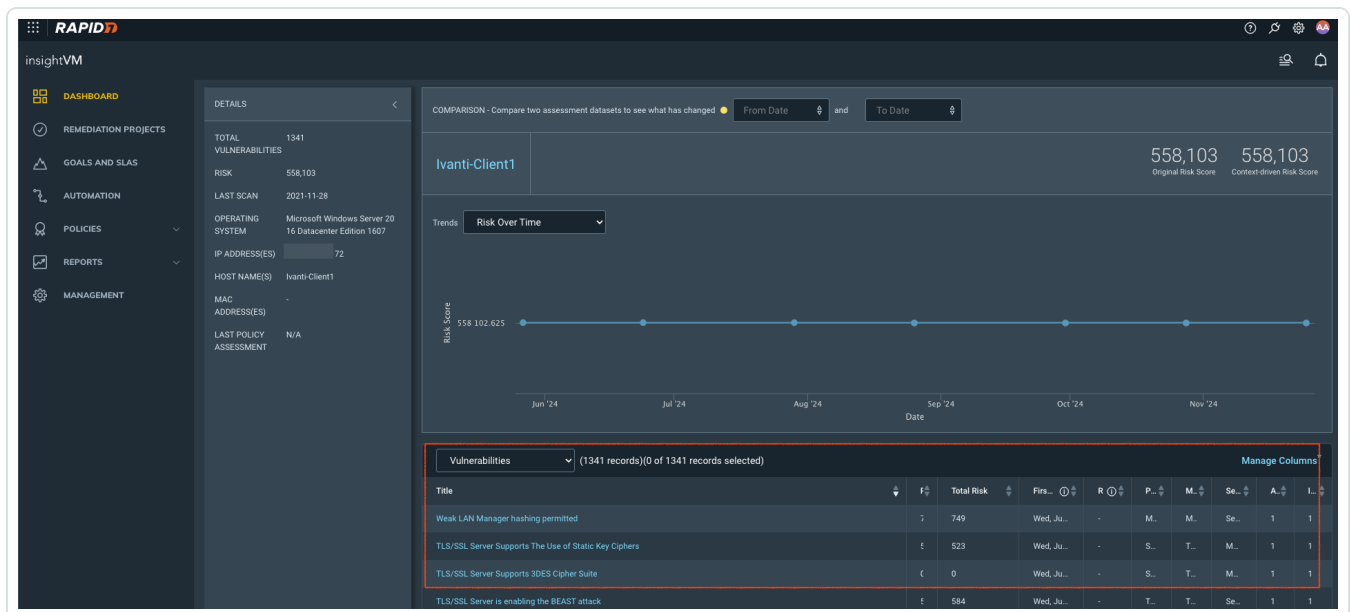
In Rapid7 InsightVM Cloud:



1. Navigate to **Dashboard > Newly Discovered Assets** page.



2. Click on any asset name.

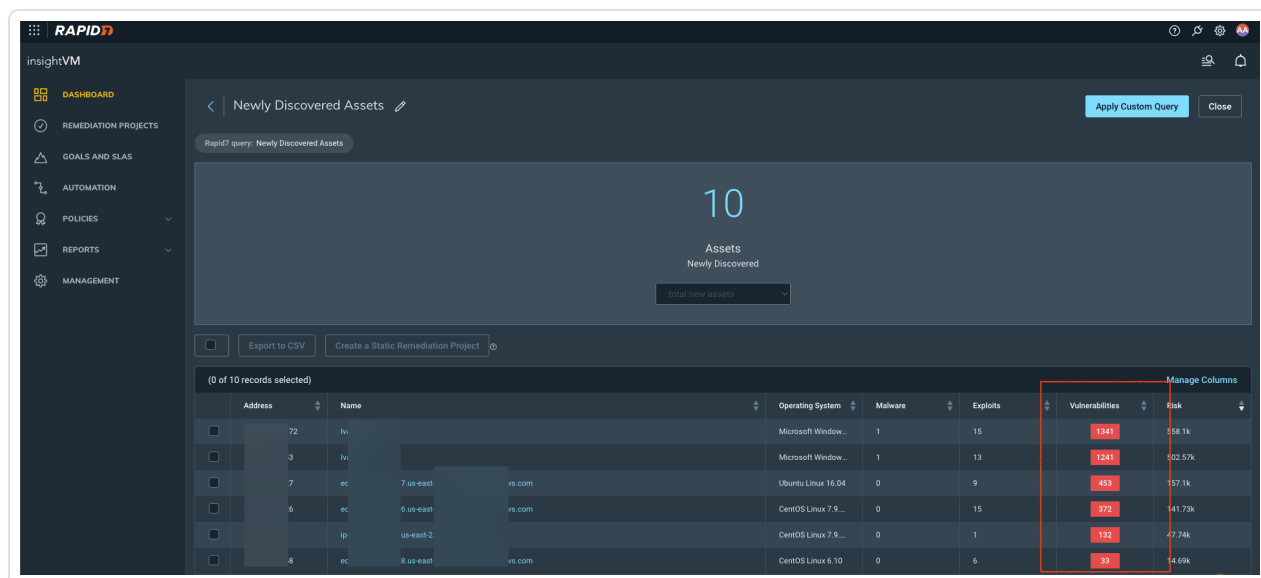


3. To validate the number of findings:

- Perform a query using the API and refer to the findings count in the new response field.



- The count displayed in the UI may not reflect the actual ingested data. The values highlighted in the following image differ from the numbers retrieved via the API.



In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between Rapid7 InsightVM Cloud and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Rapid7 InsightVM Cloud and Exposure Management should match.

**Important!** The number of findings displayed in the Rapid7 InsightVM Cloud user interface may not match the number retrieved via the API. Exposure Management aligns with the findings count provided in the API response.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed (status = NOT\_VULNERABLE) and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears in the scan findings.
- The finding no longer appears because its related asset was archived.



**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## RedHat Insights Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Red Hat® Insights](#) continuously analyzes platforms and applications to predict risk, recommend actions, and track costs so enterprises can better manage [hybrid cloud environments](#). Insights is included with almost every subscription to [Red Hat Enterprise Linux®](#), [Red Hat OpenShift®](#), and [Red Hat Ansible® Automation Platform](#).

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">Red Hat® Insights</a>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

### Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:



- **Generate RedHat Client ID and Secret:**

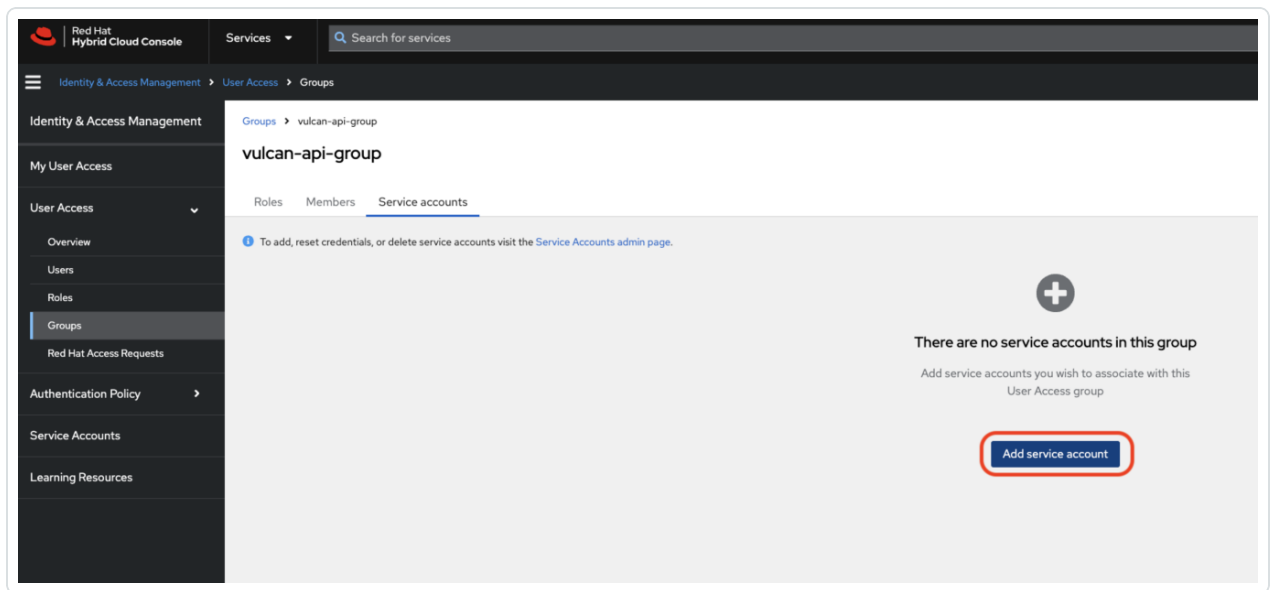
1. Navigate to the Red Hat Console at <https://console.redhat.com/iam>.
2. Navigate to **Service Accounts** and click on **Create service account**.
3. Type a **Service Account Name** and provide a **Short Description** for the account.
4. Click **Create**.
5. Save the **Client ID** and **Client secret**, as you won't be able to view them again. Check the box indicating you have done so and click **Close**.

- **Create a Redhat Group with the required access permissions:**

1. Navigate to **User Access > Groups** and select **Create group**.
2. Type a **Group Name** (e.g. 'em-api-group').
3. Click **Next**.
4. In the roles assignment step, in the search box, type **viewer**, and select the appropriate [API roles](#):
  - Inventory Host viewer
  - Vulnerability viewer
  - Patch viewer
5. Click **Next**.
6. On the **Add members** page, click **Next**.
7. On the **Review details** page, click **Submit**.
8. Click **Exit**.

- **Assign the Service Account to your Group:**

1. Within the **Groups** section, click on the newly created group name.
2. Navigate to the **Service Accounts** tab > **Add service account**.



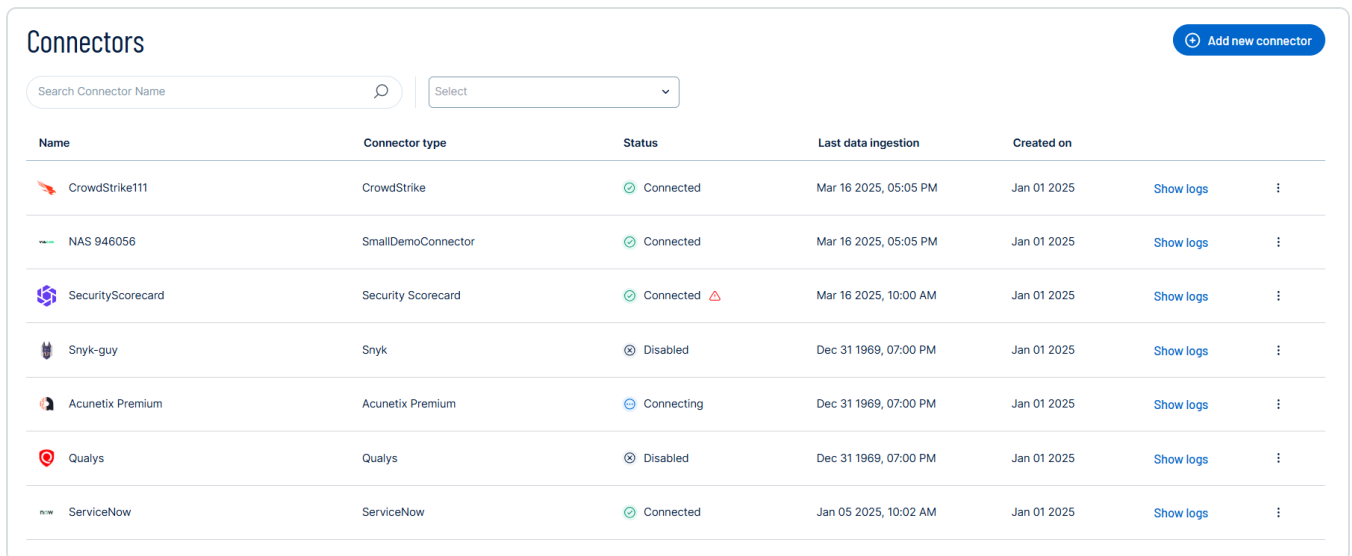
3. Locate the service account you created earlier and select it by checking the box next to its name.
4. Click **Add to group**.

## Add a Connector

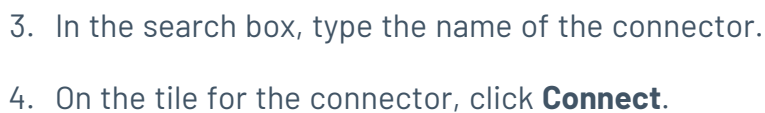
To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.



- The **Connector Library** appears.



## Configure the Connector



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Client ID** and **Client Secret** text boxes, paste the client credentials you generated in Red Hat.
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) From the drop-down menu, you can choose to automatically remove assets that reach a certain asset status, for example, **Stale**.
5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
    - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
    - If the connectivity test fails, an error message with details about the issue appears.





Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

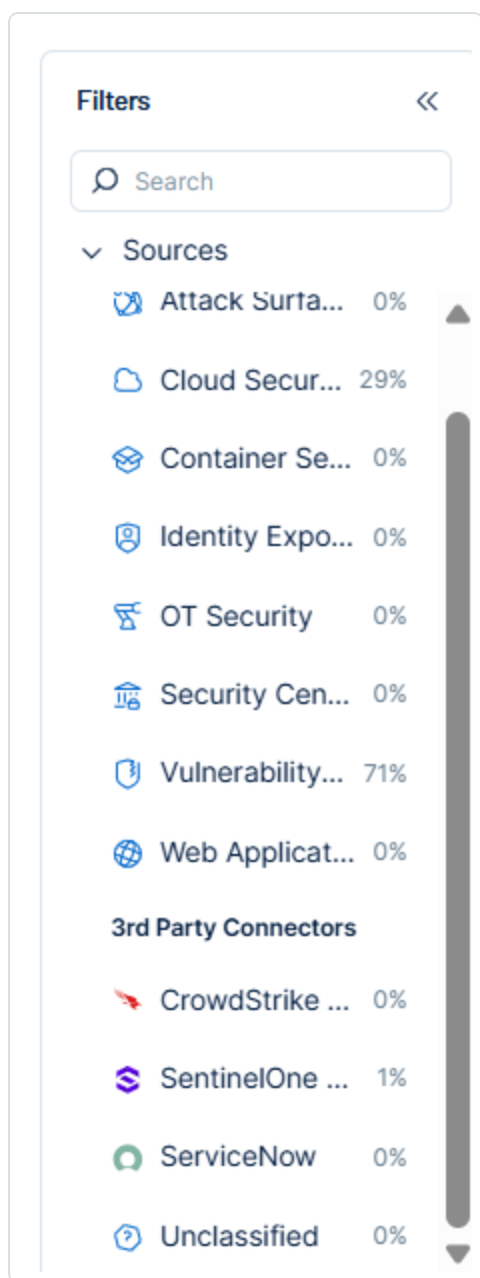
## Red Hat Insights in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

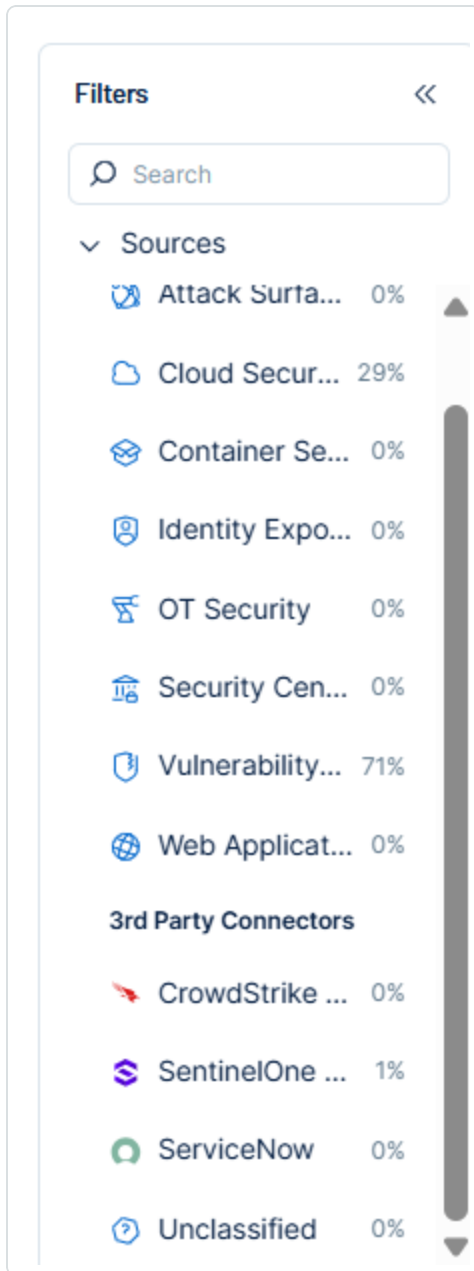
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

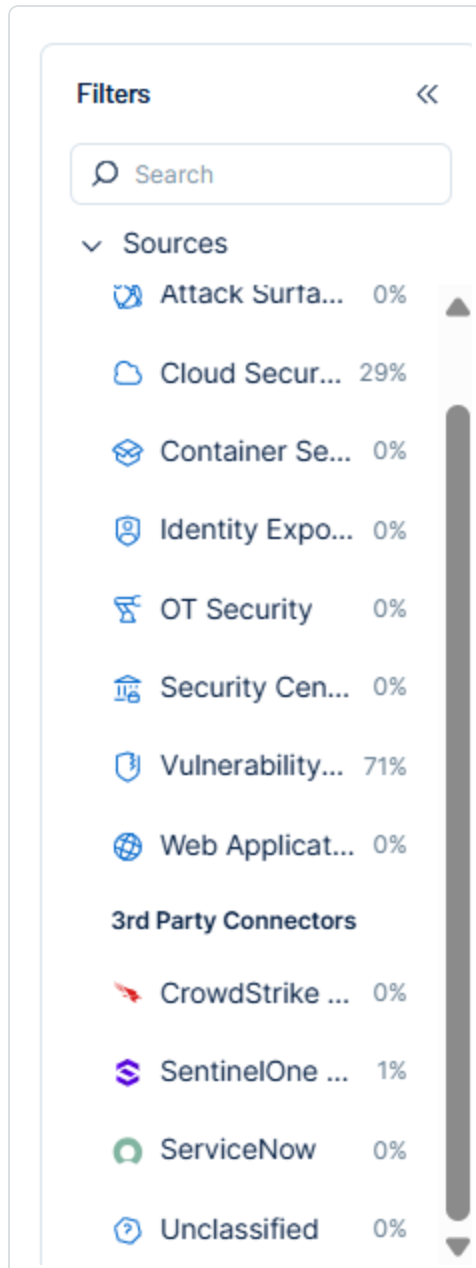
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	RedHat Insights Field
Unique Identifier	id
Asset - Name	display_name
Asset - Operating Systems	system_profile.operating_system.name
Asset - IPv4 Adresses	ip_addresses
Asset - IPv6 Adresses	
Asset - First Observation Date	created
Asset - Last Observed At	Asset - Last Observed At updated
Asset - Host Fully Qualified DNS	fqdn
Asset - MAC Addresses	mac_addresses
Asset - External Tags	attributes.tags groups.name
Asset Custom Attributes	"redhat_uuid": id "ansible_hostname": "ansible_host or fqdn "system_state": systemd.state, "infrastructure_type": system_



	<pre>profile.infrastructure_type  "cloud_provider": system_profile.cloud_provider,  "bios_vendor": system_profile.bios_vendor,  "system_memory_bytes": system_profile.system_memory_bytes</pre>
--	---

## Finding Mapping

Tenable Exposure Management UI Field	RedHat InsightsField
Unique Identifier	asset id + unique vulnerability id
Finding Name	cve_id
CVEs	cve_id
Severity Driver	cvss3_score
Description	description
First Seen	first_reported
Last seen (Observed)	last_evaluation
Finding Custom Attributes	<pre>rule_id  rule_description  rule_error_key  rule_vulnerability  public_date  impact  business_risk</pre>

## Finding Status Mapping

Tenable Exposure	RedHat Insights Status
------------------	------------------------



Management Status	
Active	Not Reviewed (0), In-Review (1), On-Hold (2), Scheduled for Patch (3), No Action - Risk Accepted (5)
Fixed	Resolved (4), Resolved via Mitigation (e.g. done without deploying a patch)(6)

**Note:**For **RedHat Insights**, Exposure Management uses the `status_id` field to determine finding status.

## Finding Severity Mapping

Tenable Exposure Management Severity	ReHat Insights Score
Critical	<b>CVSS:</b> 9.0 - 10.0
High	<b>CVSS:</b> 7.0 - 8.9
Medium	<b>CVSS:</b> 4.0 - 6.9
Low	<b>CVSS:</b> 1-3.9
None	<b>CVSS:</b> 0

**Note:**For **RedHat Insights**, Exposure Management uses the `cvss3_score` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>



	<ul style="list-style-type: none"><li>Asset status changes to one of the selected statuses defined in the Asset Retention configuration.</li></ul> <div><b>Note:</b> By default, no status is selected. Users can choose to archive assets based on status in the <a href="#">connector setup page</a>.</div>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding status changes to Not Reviewed (0), In-Review (1), On-Hold (2), Scheduled for Patch (3), or No Action - Risk Accepted (5) on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## API Endpoints in Use

```
/api/inventory - v1  
/api/vulnerability - v1  
/api/patch - v3
```

API	Use in Tenable Exposure Management	Required Permissions
<a href="https://sso.redhat.com/auth/realms/redhat-external/protocol/openid-connect/token">https://sso.redhat.com/auth/realms/redhat-external/protocol/openid-connect/token</a>	Authentication	-
<a href="#">/api/inventory/v1/hosts</a>	Assets	Inventory Hosts Viewer
<a href="#">/api/vulnerability/v1/vulnerabilities/cves</a>	Detections	Vulnerability viewer
<a href="#">/api/vulnerability/v1/cves/{{cve_id}}/affected_systems</a>	Additional asset data Findings	Vulnerability viewer

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the RedHat Insights platform.



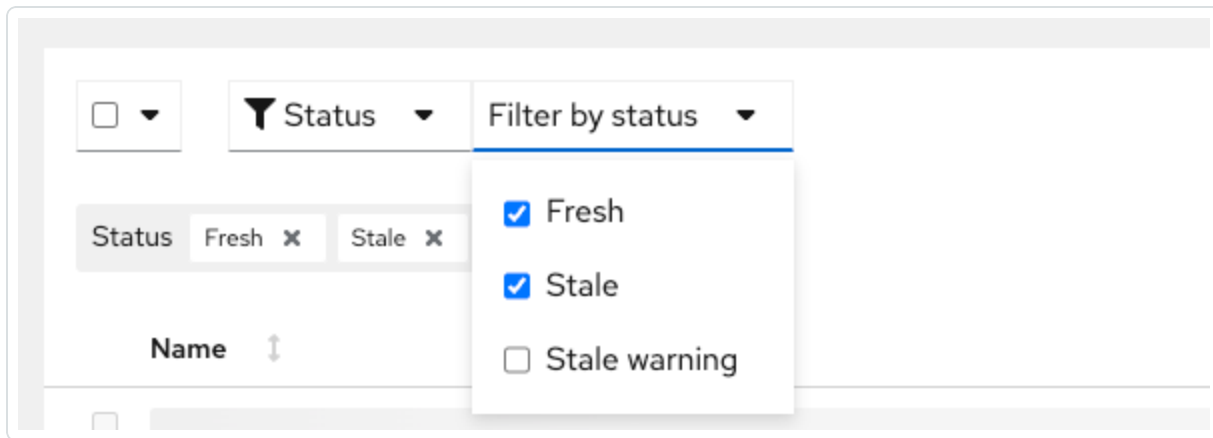


## Asset Data Validation

**Objective:** Ensure that the number of assets in RedHat Insights aligns with the number of assets displayed in Exposure Management.

In RedHat Insights:

1. Navigate to **Inventory > Systems**.
2. Review the total number of systems shown.
3. If the Exposure Management connector is configured to [archive assets based on their status](#), ensure all status types are selected during validation.



In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between RedHat and Tenable Exposure Management.

**Expected outcome:** All systems visible in RedHat Insights (with eligible statuses) should appear in Exposure Management. The numbers may not match if assets are archived based on status or last seen date.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset status changed to one of the selected statuses defined in the [Asset Retention](#) configuration.
- The asset was archived based on the last observed date (last seen).

## Finding Data Validation



**Objective:** Ensure that the number of findings in RedHat Insights aligns with the number of findings in Exposure Management.

In RedHat Insights (from the vulnerability perspective):

1. Navigate to **Security > Vulnerability > CVEs**.
2. Click on a specific CVE.
3. Apply the following filters:
  - **Systems:** Set to **"1 or more"**.
  - **Advisory:** Ensure no advisory filter is applied.
  - **Status:** Select the following values: **Not reviewed**, **In review**, **On-hold**, **Scheduled for patch**, and **No Action - Risk Accepted**.

Red Hat's policy requires displaying all high priority, critical, and important CVEs regardless of Advisory status

The screenshot shows the Red Hat Insights interface for CVEs. At the top, a blue banner states: "Red Hat's policy requires displaying all high priority, critical, and important CVEs regardless of Advisory status". Below this, there are filter controls. On the left, a "Systems" filter is set to "1 or more". In the center, a "Status" filter dropdown is open, showing a list of status options: "Not reviewed" (checked), "In review" (checked), "On-hold" (checked), "Scheduled for patch" (checked), "Resolved" (unchecked), "No action - risk accepted" (unchecked), and "Resolved via mitigation" (unchecked). To the right of the status filter, there are buttons for "In review", "On-hold", and "Shc". Below the filters, a table displays CVEs. The table has columns for "CVE ID" and "Severity". The first four rows show CVEs with "Important" severity: CVE-2023-3972, CVE-2023-5678, CVE-2023-5178, and CVE-2023-38545. The fifth row shows a CVE with "Low" severity.

CVE ID	Severity
CVE-2023-3972	Important
CVE-2023-5678	Important
CVE-2023-5178	Important
CVE-2023-38545	Important
	Low



All systems affected by the CVE are displayed. These represent the finding connections.

The screenshot shows the Red Hat Insights interface for CVE-2023-3972. The left sidebar contains navigation links: Dashboard, Inventory, Content, Operations, Security (with sub-links for Vulnerability, CVEs, Reports, and Systems), Compliance, Malware, Business, Automation Toolkit, and Register Systems. The main content area displays the CVE details, including its publish date (01 Nov 2023), a description of the vulnerability, and a CVSS 3.0 base score of 7.8. Below this, a table lists affected systems. The table has columns for Name, Group, Tags, OS, Advisory, Status, Last seen, and Remediation. One system is listed: ip-...internal, group test\_group, OS RHEL 9.2, with advisory RHSA-2023-6282 and status In review.

In RedHat Insights (from the asset perspective):

1. Navigate to **Inventory > Systems**.
2. Click on a specific system.
3. Click on the **Vulnerabilities** tab.
4. Ensure no advisory filter is *not* applied.

All CVEs affecting the system are displayed. These represent the system's findings.

The screenshot shows the Red Hat Insights interface for a specific system's vulnerabilities. The left sidebar is the same as the previous screenshot. The main content area shows the system details (ip-...internal) and a table of vulnerabilities. The table has columns for CVE ID, Publish date, Severity, CVSS base score, Advisory, Business risk, Status, and Remediation. Five vulnerabilities are listed, including CVE-2023-3972, CVE-2023-38545, CVE-2023-5345, and CVE-2023-4527.

In Tenable Exposure Management:

1. [Locate your connector findings.](#)
2. Compare the total number of findings between RedHat Insights and Tenable Exposure Management.



**Expected outcome:** The total numbers returned in RedHat Insights and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## RiskRecon Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[RiskRecon](#) provides you with the visibility and tools you need to make third-party cyber risk decisions and take action at the speed of business.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">RiskRecon</a>
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)

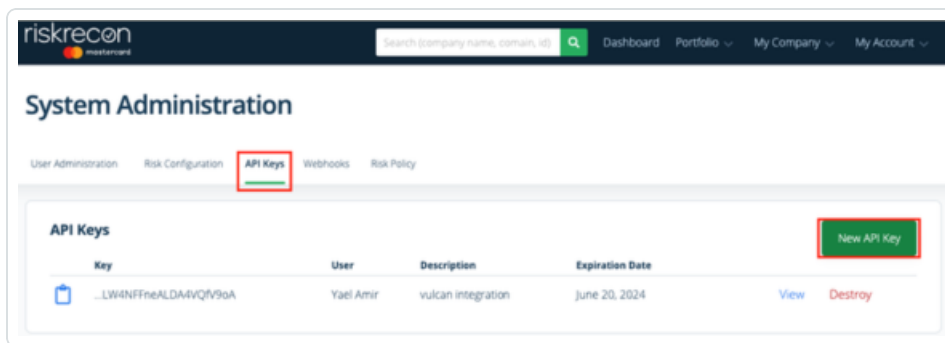


Supported version and type	SaaS (latest)
----------------------------	---------------

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Generate a RiskRecon API Token:**
  1. In the RiskRecon platform, navigate to **My Account > System Administration**.
  2. Click **API Keys** and then **New API Key**.



3. Type a brief **Description** and set the **Expiration Date** to 1 year.
4. Click **Create API Key**.
5. Save the generated API Key for later use with Tenable Exposure Management.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.
















Connectors

Search Connector Name

Select

+

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <div></div>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <div></div>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <div></div>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <div></div>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <div></div>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <div></div>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <div></div>

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

DAST

Connect

Acunetix Premium

DAST

Connect

Aqua CWPP

CWPP

Connect

Armis

OT

Connect

AWS Config

EDR

Connect

AWS EC2

Asset Inventory

Connect

AWS Security Hub Standards

Connect

Axonius

Connect

Azure

Connect

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

Configure the Connector



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Key** text box, paste the API key you [generated in RiskRecon](#).
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - **To fetch specific companies instead of all companies:** By default, the **Fetch all companies (auto-update for new additions)** check box is selected. To choose specific companies, clear this check box. When the drop-down appears, select the RiskRecon companies you want to include.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.



Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

✔ Successful tests 3 out of 4 integration tests succeeded

[Test connectivity](#)

Show tests ▼

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## RiskRecon in Tenable Exposure Management

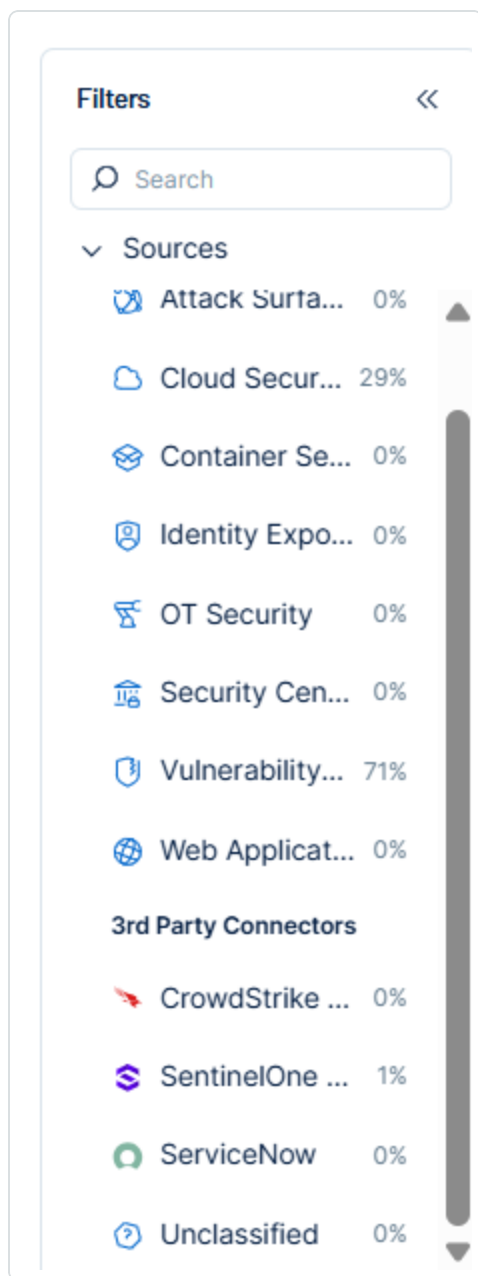
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.





The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

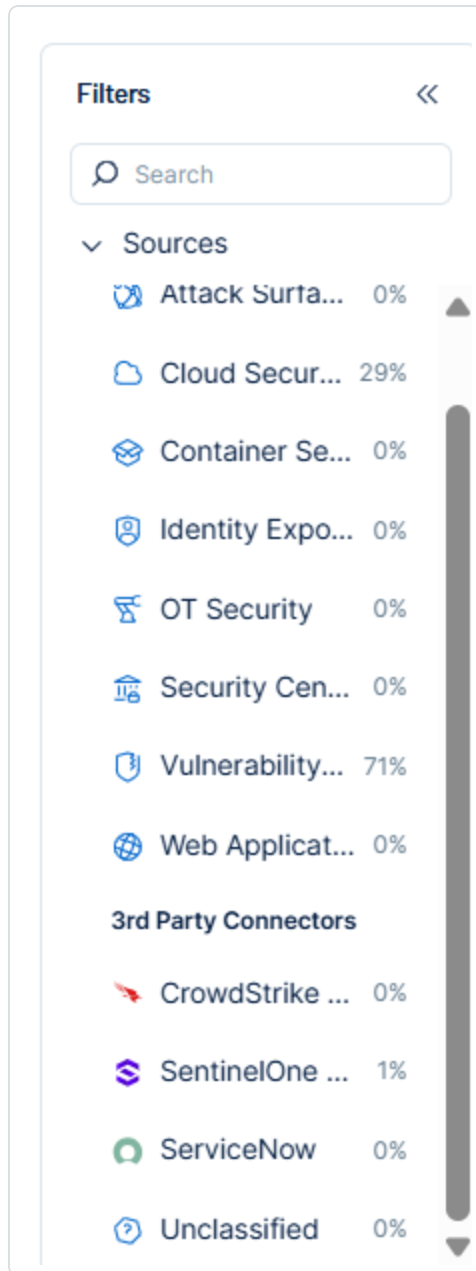
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

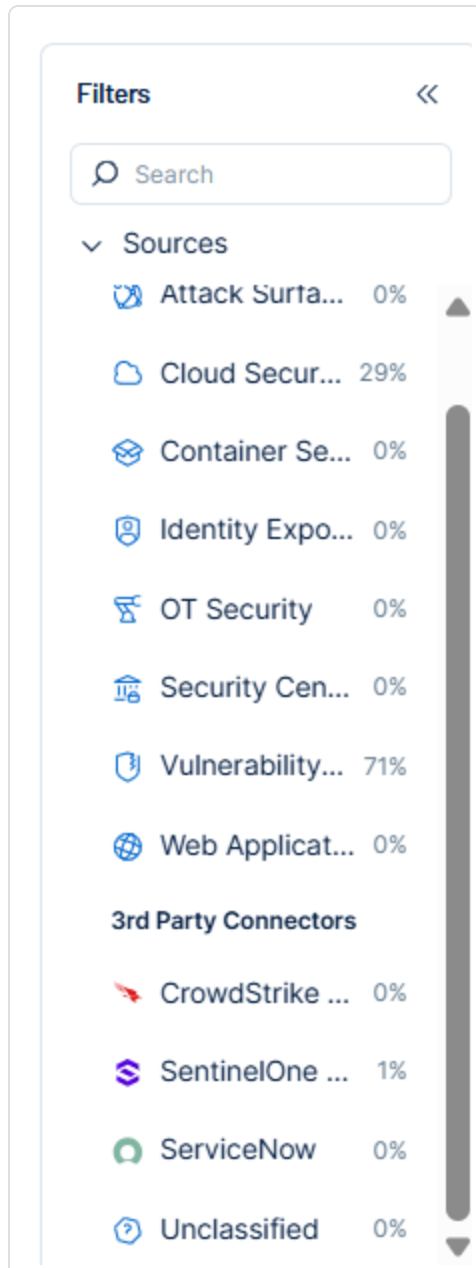
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management Value	RiskRecon Filed
Unique Identifier	host_name or ip_address or domain_name
Asset - Name	host_name or ip_address or domain_name
Asset - Last Observed At	record_load_timestamp or last_seen
Asset - Webapp Homepage Screenshot Url	host_name or ip_address or domain_name
Asset - External Tags	company name hosting_provider asset_value domain country_name
Asset Custom Attributes	hosting_provider asset_value auth_detected (has authentication) host_name domain_name ip_address country_name



## Finding Mapping

Tenable Exposure Management UI Field	RiksRecon Field
Unique Identifier	asset id + finding_id + unique vulnerability id
Finding Name	display_name
Description	<ul style="list-style-type: none"><li>• Vulnerability: ssue_long_vuln or issue_short_vuln</li><li>• Introduction: issue_long_intro or issue_short_intro</li><li>• EOL: issue_long_eol or issue_short_eol</li></ul>
Severity Driver	attributes.severity
First Seen	first_seen
Last seen (Observed)	last_seen
Finding Custom Attributes	finding_id finding_detail finding_data_value finding_extra_data_value asset_value priority severity ip_address host_name domain_name severity

## Finding Status Mapping



Tenable Exposure Management Status	RiskRecon Status
Active	All findings returned from the connector
Fixed	Otherwise

**Note:**For **XCONNECTOR**, Exposure Management uses the X field to determine finding status. If X is not available, Exposure Management uses the Yfield from the connector, if provided.

## Finding Severity Mapping

Tenable Exposure Management Severity	RiskRecon Score
Critical	<b>Severity:</b> Critical
High	<b>Severity:</b> High
Medium	<b>Severity:</b> Medium
c	<b>Severity:</b> Low

**Note:**For **XCONNECTOR**, Exposure Management uses the `attributes.severity` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	Asset that appears in Exposure Management and is not returned on the next connector sync
Change a Finding status from "Active" to "Fixed"	Finding no longer appears in the scan findings



**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	host_name or ip_address or domain_name
Finding	asset_id + finding_id + unique vulnerability_id
Detection	security_criteria

## API Endpoints in Use

API version: 0.0-1.0

API	Use in Tenable Exposure Management
/v1/toes	Get TOE_IDs (vendor ids) and vendor names
/v1/hosts/{toe_id}	Assets
/v1/findings_paginated/{toe_id}	Findings
/v1/display_names/security_criteria	Detections, Solutions
/v0/cpe/raw_language?language=english&security_criteria={security_criteria}	Detections

## Support Limitations and Expected Behavior



This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

## Company Selection

The connector allows users to select which companies to ingest into Exposure Management. Only data related to the selected companies will be synchronized.

## Findings Ingestion Criteria

- **Status filtering:** Findings with a status of Pass or Positive are excluded from ingestion.
- **Finding count differences:** RiskRecon counts findings based on a combination of issue + IP. For example, if a device has two IP addresses and one issue, RiskRecon will count this as two findings. In contrast, Exposure Management counts findings by issue alone, regardless of IP associations. As a result, RiskRecon may display a higher total number of findings.

[Return to Security Profile](#)

### Software Patching

Security Criteria	Rating	Issue Count	Population	Issue Rate			
Application Server Patching	<span>B</span> 7.3	10	254	4%	<a href="#">View Details</a> <span>▼</span>		
OpenSSL Patching	<span>A</span> 10	0	8	0%	<a href="#">Hide Details</a> <span>▲</span>		
RiskRecon observed no systems running end-of-life OpenSSL software. Maintaining software at the current, supported patch levels helps eliminate known vulnerabilities that could be exploited to compromise the system.							
CMS Patching	<span>F</span> 2.9	4	20	20%	<a href="#">Hide Details</a> <span>▲</span>		
RiskRecon observed 4 systems running end-of-life content management systems that have known security vulnerabilities. RiskRecon suggests prioritizing remediation of the issues in order of the assigned issue risk priority. The highest priority issues are rated as critical under the CVSS scheme and exist in high value assets. The importance of addressing the lower risk priority issues, such as low and medium severity issues in idle and low value systems, should be evaluated on a case-by-case basis.							
Software	IP Address	Hostname	Days Open	Asset Value	Severity	Priority	Action Plan
<span>+</span> WordPress 5.2.0-5	1	ma	752	high	critical	1	Yes
<span>+</span> WooCommerce 3.6.4	3	ww	1	high	high	2	Yes
<span>+</span> WordPress 5.9.1	3	ww	546	high	medium	3	Yes
<span>+</span> Drupal 6	1	em	2056	high	critical	1	Yes
<span>+</span> Drupal 6	1	em	45	high	critical	1	Yes
<span>+</span> WordPress 5.7.1	1	dev	45	medium	critical	2	Yes





- **Security criteria without identifiers:** RiskRecon Security Criteria that do not disclose IP addresses, hosts, or domains are not ingested into Exposure Management. Therefore, RiskRecon may show a higher number of unique vulnerabilities than Tenable.

Security Criteria	Rating	Issue Count	Population	Issue Rate	
CMS Authentication	C 6.0	3	14	21%	<a href="#">View Details</a> ▼
HTTP Security Headers	C 6.7	1,348	1,496	90%	<a href="#">View Details</a> ▼
External Threat Intelligence Alerts	Info	0	n/a	n/a	<a href="#">View Details</a> ▼
High Value System Encryption	C 6.2	8	261	3%	<a href="#">View Details</a> ▼
Malicious Code	A 10	0	n/a	n/a	<a href="#">View Details</a> ▼

## Asset Count Differences

- **Asset type mapping:** RiskRecon displays only hosts in its asset view. However, findings may also be linked to IP addresses or domains. In Exposure Management, each IP or domain is treated as a distinct asset, which may lead to a higher number of assets displayed in Tenable.
- **Domain ownership filtering:** RiskRecon filters out hosts that are not part of the company's owned domains. Exposure Management does not apply this filter and displays all hosts, regardless of domain ownership. This may result in displaying a higher asset count on Exposure Management.
- **Security criteria without identifiers:** RiskRecon Security Criteria that do not disclose IP addresses, hosts, or domains are not ingested into Exposure Management. Therefore, RiskRecon may show a higher number of unique vulnerabilities than Tenable.



Security Criteria	Rating	Issue Count	Population	Issue Rate	
CMS Authentication	C 6.0	3	14	21%	<a href="#">View Details</a> ▼
HTTP Security Headers	C 6.7	1,348	1,496	90%	<a href="#">View Details</a> ▼
External Threat Intelligence Alerts	Info	0	n/a	n/a	<a href="#">View Details</a> ▼
High Value System Encryption	C 6.2	8	261	3%	<a href="#">View Details</a> ▼
Malicious Code	A 10	0	n/a	n/a	<a href="#">View Details</a> ▼

## Hierarchy Display Limitation

In the RiskRecon host issues tab, the displayed value is the Security Profile, which is the parent hierarchy of the Security Criteria (the equivalent of a unique vulnerability in Exposure Management). As a result, the view may not reflect specific issue-level detail.

OverviewSecurity ProfileIT ProfileAction PlanPDF / Data DownloadsBenchmark

Return to IT Profile

Hosts

2,464Hostnames

2,464Total

Web 2,313DNS 30Email 121

Hostnames

Hostname

3dc.com

3dc

3dd.a.com

3dd

3ddn

3dnla.com

Host ProfileHost Issues

Host Summary

Hostname3IP Address3.Hosting ProviderGoogle, Inc.

Hosting Typeexternal

Software Patching

Issue	Detail	Severity	Priority
software	Apache 2.2.0	critical	3

Web Encryption

Issue	Detail	Severity	Priority
certificate	certificate subject	medium	5
certificate	supported ciphers	medium	5

Application Security

Issue	Detail	Severity	Priority
software	Missing Security Headers	low	6



## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the **RiskRecon** platform.

### Asset Data Validation

**Objective:** Because RiskRecon doesn't provide an option to view all assets for all companies, RiskRecon and Tenable Exposure Management don't show the same number of assets in the UI. In order to compare the data with Tenable Exposure Management, you must compare one company at a time. The numbers calculated this way should be identical within both RiskRecon and Tenable Exposure Management.

In RiskRecon:

1. Navigate to the **Portfolio** tab and choose the target company.
2. Navigate to the **PDF / Data Downloads** tab.

The screenshot shows the RiskRecon interface for 'A-Z Bus Sales, Inc.'. The top navigation bar includes a search bar and links to Dashboard, Portfolio, My Company, and My Account. The main content area is titled 'A-Z Bus Sales, Inc.' and shows an assessment date of Jan 13, 2024. Below this, there are tabs for Overview, Security Profile, IT Profile, Action Plan, PDF / Data Downloads (selected), Benchmark, Company Profile, and Compliance. The 'Data Files' section is active, displaying a table with columns: Name, Description, and File Type. The table lists a file named 'Hosts' with a detailed description of the host enumeration process. A 'CSV' download button is visible next to the file.

3. Scroll down to the **Data Files** section.
4. Download each available data file, except for the **Owned Netblocks** file, which is not required.
5. For each downloaded file, extract the column that represents the asset.
6. Combine all extracted asset values into a single column in a new spreadsheet.
7. Remove any duplicate entries from the combined column.

The result is a deduplicated list of all assets identified for that company in RiskRecon.

In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between RiksRecon and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in RiskRecon and Exposure Management should align after taking into consideration that issues described in the [Support Limitations and Expected Behavior](#) section.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived because it did not return in the connector's next sync.

**Tip:** To learn more on how assets and findings change status, see [RiskRecon Connector](#).

## Finding Data Validation

**Objective:** Understand how RiskRecon issues are represented in Tenable Exposure Management, and why finding counts may not match between platforms.



As described in the [Support Limitations and Expected Behavior](#) section, RiskRecon and Exposure Management don't show the same number of findings in the UI. Exposure Management doesn't ingest RiskRecon issues (findings) whose status is `pass` or `positive`.

Furthermore, RiskRecon issues are counted by `issue + IP`. That means that a host with with two IPs and an issue would be counted as two issues. Exposure Management counts only the issues, without taking into account the IPs. Potentially, RiskRecon may show a higher number.

Due to these factors, there is no feasible way to validate the number of findings by using the UI.

## SecurityScorecard Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[SecurityScorecard](#) is a comprehensive cyber security risk ratings platform that continuously monitors the cyber security health of organizations to inform on cyber security risk management. SecurityScorecard identifies public-facing vulnerabilities that create a security risk.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

### Connector Details

Details	Description
Supported products	<a href="#">SecurityScorecard</a> Security Ratings
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version	SaaS (latest)

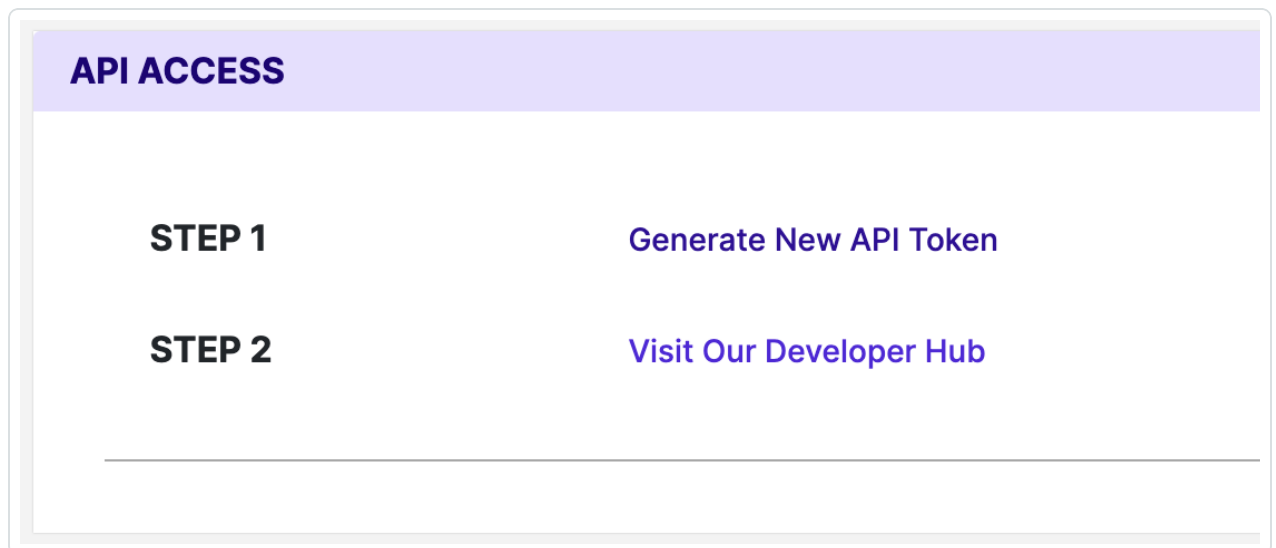


and type

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Generate a SecurityScorecard API Key:**
  1. In your **SecurityScorecard** platform, navigate to **Account > My Settings**.
  2. Click **API**.
  3. Click **Generate New API Token > Confirm**.



Save the API Key in a secure location. You will need the key later when you configure the connector in the Exposure Management platform.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **API Key** text box, paste the API key you [generated in SecurityScorecard](#).
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector. For SecurityScorecard, you must enable one of the following two options:
  - To ingest data from all domains (portfolios), select the **Always fetch all portfolios** check box.
  - Your primary SecurityScorecard domain is always ingested by default. To ingest additional domains, click **Load portfolios** and select the relevant portfolios.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears.





Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

✔ Successful tests 3 out of 4 integration tests succeeded

[Test connectivity](#)

Show tests ▼

Show tests ▼

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

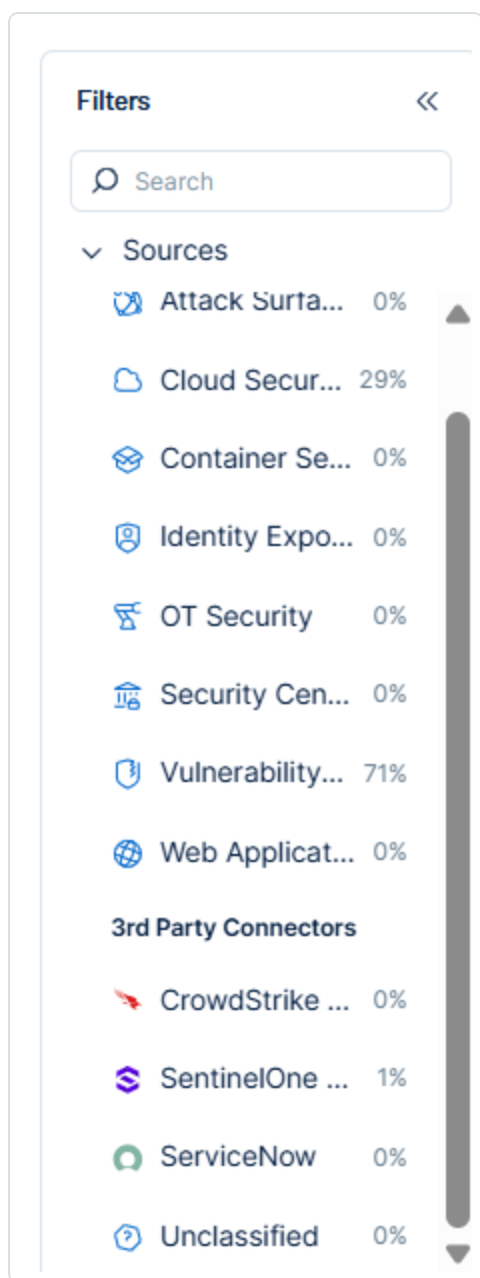
## SecurityScorecard in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

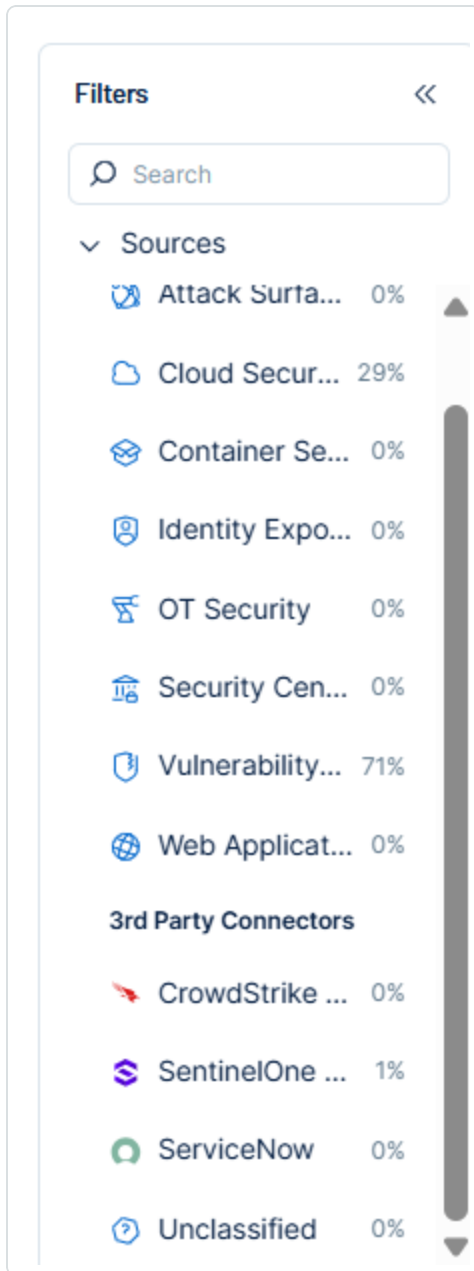
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

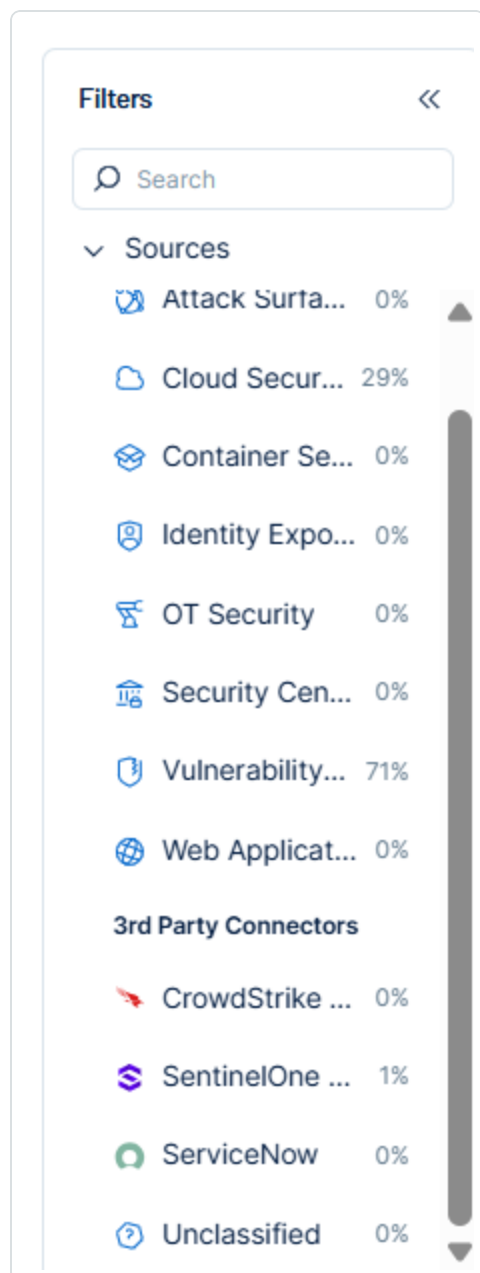
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Web Application Mapping

Tenable Exposure Management UI Field	SecurityScorecard Field
Unique Identifier	domain
Asset - Name	domain
Asset - First Observation Date	created_at
Asset - Webapp Homepage Screenshot Url	domain
Asset - External Tags	scorecard-tags
Asset Custom Attributes	security_scorecard_score security_scorecard_last_30_days_score_change security_scorecard_industry

## Finding Mapping

Tenable Exposure Management UI Field	SecurityScorecard Field
Unique Identifier	issue_type + domain + issue_id
Finding Name	title
Severity Driver	severity



Description	<code>short_description</code>
First Seen	<code>first_seen_time</code>
Last seen (Observed)	<code>last_seen_time</code>
Finding Custom Attributes	<code>issue_id</code> <code>domain</code> or <code>final_url</code> or <code>url</code> <code>vulnerability_id</code> <code>observations</code> <code>issue_score_impact</code> <code>port</code> <code>vulnerability_description</code> or <code>product_state_status_description</code> <code>long_description</code> <code>security_scorecard_score_factor</code> : <code>factor</code> <code>security_scorecard_issue_key</code> : <code>measurement_name</code> <code>security_scorecard_severity</code> : <code>severity</code>

## Finding Status Mapping

Tenable Exposure Management Status	SecurityScorecard Status
Active	All other statuses, including: <code>false_positive</code> <code>misattribution</code> <code>compensating_control</code>
Fixed	<code>technical_remediation</code>

**Note:**For SecurityScorecard, Tenable uses the `feedback_type` field to determine status.

## Finding Severity Mapping



Tenable Exposure Management Severity	SecurityScorecard Score
Critical	high
High	medium
Medium	low
Low	info

**Note:** For SecurityScorecard, Tenable uses the `severity` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>- Asset not seen for X days according to <b>Last Seen</b>. See <a href="#">Asset Retention</a></li><li>- Asset that appears in Tenable Exposure Management and isn't returned on the next connector sync</li></ul>
Change of a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>- Finding no longer appears in the scan findings</li><li>- Finding status changes to <code>technical_remediation</code> on the vendor side</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria



Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	domain
Finding	domain + issue_type + issue_id
Detection	issue_type

## API Endpoints in Use

API	Use in Tenable Exposure Management
<code>https://api.securityscorecard.io/myself</code>	Assets
<code>https://api.securityscorecard.io/companies/{{main_company.domain}}</code>	Assets
<code>https://api.securityscorecard.io/companies/{{main_company.domain}}/factors</code>	Assets
<code>https://ui-metadata.securityscorecard.io/metadata/issue-types/{{issue_type}}.json</code>	Detections Solutions
<code>https://api.securityscorecard.io/companies/{{ main_details.domain }}/issues/{{ issue_type }}/</code>	Findings
<code>https://api.securityscorecard.io/portfolios</code>	Assets
<code>https://api.securityscorecard.io/portfolios/{{ portfolio }}/companies</code>	Assets





<code>https://api.securityscorecard.io/scorecard-tags</code>	Tags
<code>https://api.securityscorecard.io/scorecard-tags/{{tag.id }}/companies</code>	Tags

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Portfolios and Data Ingestion

- When setting up the connector, the user can select specific portfolios for ingestion.
- A **Pull All Portfolios** checkbox is available. When enabled, the connector automatically ingests data from all portfolios.
- Companies and associated domains within the selected portfolios are ingested into Exposure Management.

### Limitations

- The connector does not display a company's Digital Footprint, which includes associated IPs and domains. This limitation is due to platform restrictions in Exposure Management. Only pages directly tied to vulnerabilities are displayed, even for asset-related information.
- Findings with a **Positive** severity are excluded from the ingested data.
- The connector ingests only findings generated directly by SecurityScorecard. Findings provided by third-party integrations within SecurityScorecard are not imported.

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the SecurityScorecard platform.

### Asset Data Validation

**Objective:** Ensure that the number of assets imported from SecurityScorecard aligns with the assets displayed in Exposure Management.



## In SecurityScorecard:

During connector setup, you can choose to:

- Select specific portfolios, or
- Enable the Always fetch all portfolios option.

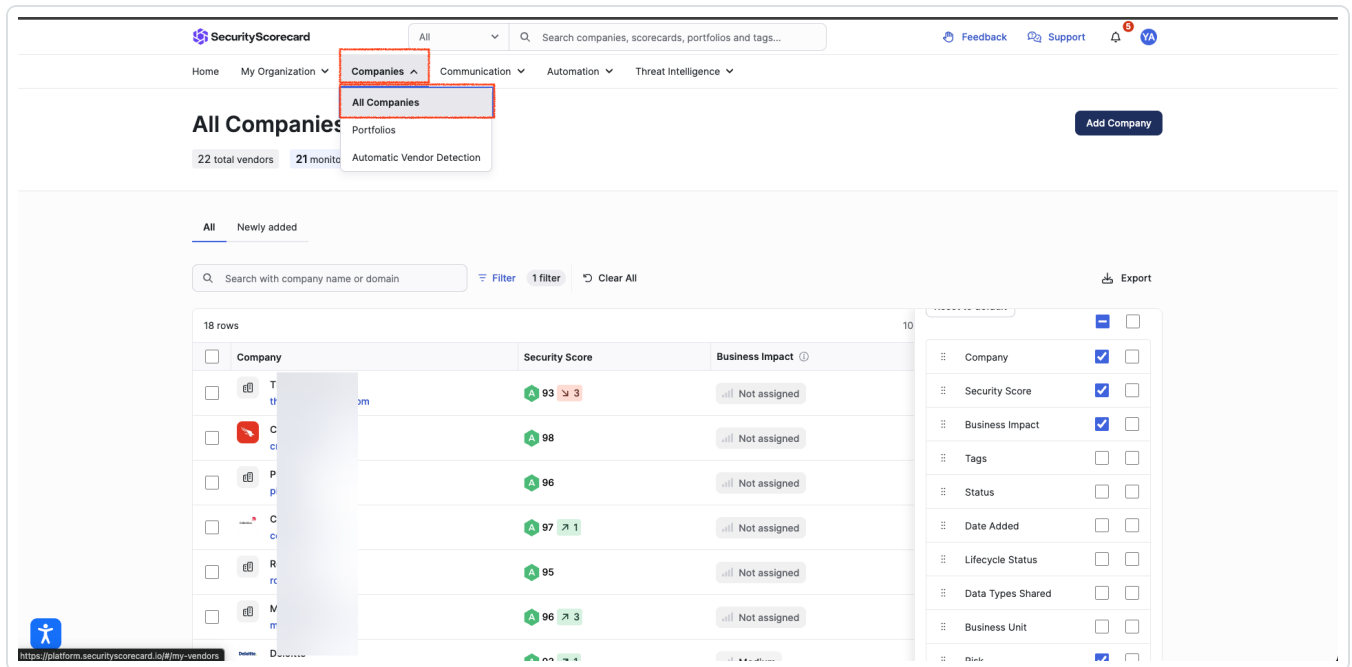
Regardless of selection, the scorecard for your own company is always imported—even if no portfolios are selected.

- If no portfolios are selected and Always fetch all portfolios is not selected, only your own company is imported.

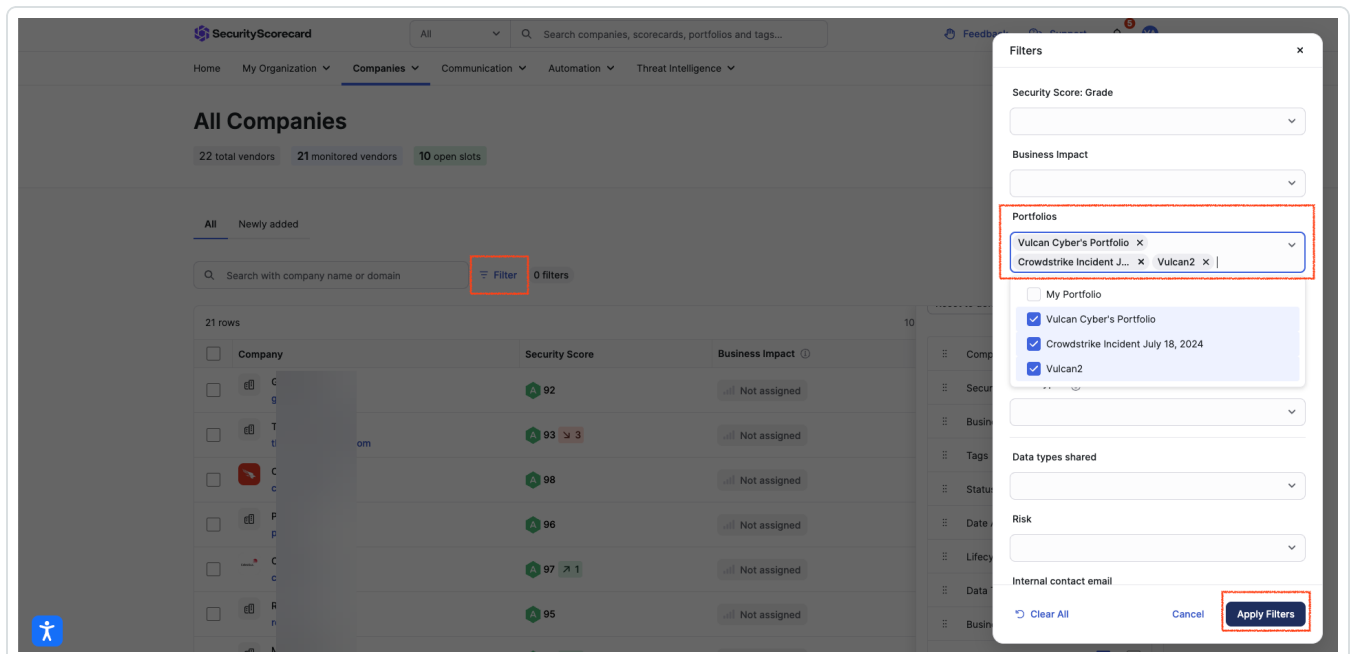
The screenshot shows the SecurityScorecard interface. The top navigation bar includes 'Home', 'My Organization', 'Companies', 'Communication', 'Automation', and 'Threat Intelligence'. The 'My Organization' dropdown is expanded, showing 'My Scorecard' and 'Trust Center'. The 'My Scorecard' section displays the 'Vulcan Cyber' scorecard with a 'Score Factors' table. The table lists various security factors and their scores.

Factor	Score	Impact	Issues	Findings
Network Security	77	10.8	6	18
Application Security	78	8.7	1	113
DNS Health	100	0.0	no issues	5
Patching Cadence	100	0.0	no issues	3
Endpoint Security	100	0.0	no issues	0

- If specific portfolios are selected, the list of companies included in those portfolios appears on the screen.



1. Apply a filter based on the selected portfolios. If **Always fetch all portfolios** is selected, ensure all portfolios are included in the filter. Private portfolios should not be included, as they are not supported.



2. Click **Apply Filter**. The number of companies expected to be imported appears.

**SecurityScorecard** All Search companies, scorecards, portfolios and tags... Feedback Support

Home My Organization **Companies** Communication Automation Threat Intelligence

**All Companies** Add Company

22 total vendors 21 monitored vendors 10 open slots

All Newly added

Search with company name or domain Filter 1 filter Clear All Export

18 rows

Company	Security Score	Business Impact
Th...	93 3	Not assigned
Cr...	98	Not assigned
Pl...	96	Not assigned
Co...	97 1	Not assigned
Re...	95	Not assigned
M...	96 3	Not assigned

Company Security Score Business Impact

Company Security Score Business Impact Tags Status Date Added Lifecycle Status Data Types Shared Business Unit

**Important!** If your own company is not part of any selected portfolio, add 1 to the count. It will be imported regardless of portfolio selection.

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between SecurityScorecard and Tenable Exposure Management.

**Expected outcome:** The asset count in Exposure Management should match the number of companies shown in SecurityScorecard, accounting for your own company if applicable.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on its last observed date (last\_seen field).
- You selected specific portfolios during connector setup, and the missing company is not part of those portfolios.
- You enabled Always fetch all portfolios, but private portfolios were selected in the filter.

**Important!** Private portfolios will not be extracted, even if selected.

Finding Data Validation

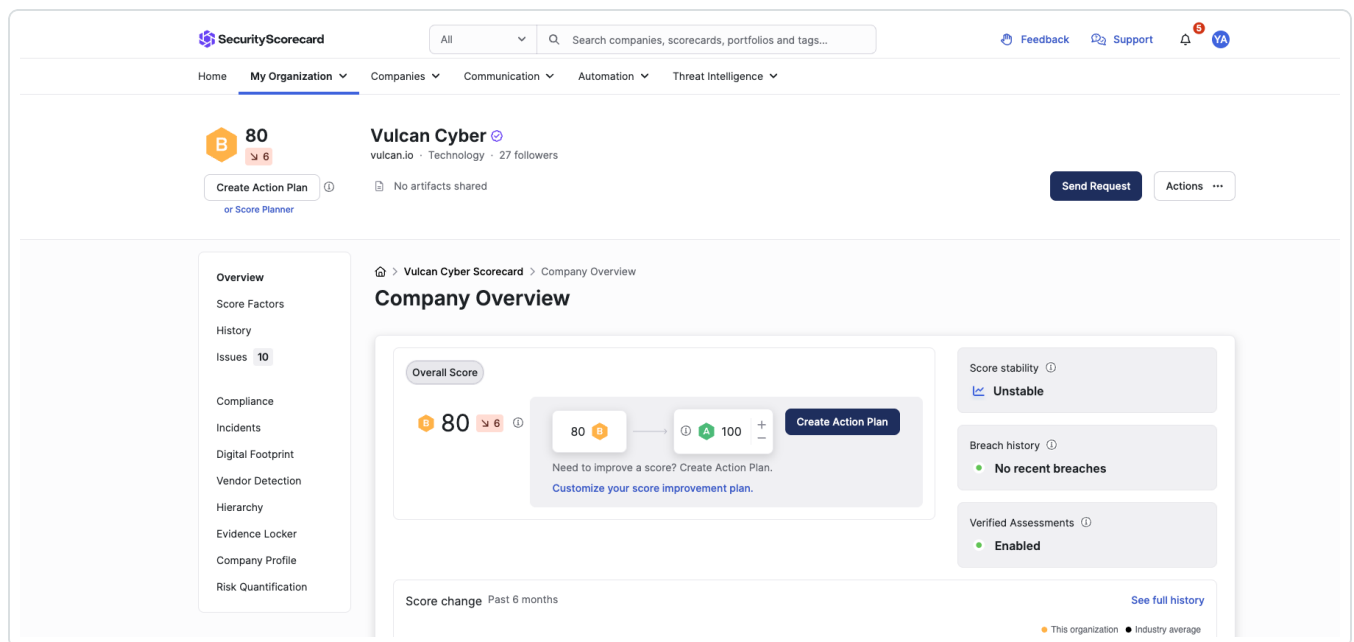


**Objective:** Ensure the number of findings in SecurityScorecard aligns with the findings displayed in Exposure Management.

In SecurityScorecard:

SecurityScorecard does not display all findings across assets in a single, consolidated view. Instead, you can validate the findings by reviewing a single asset as an example. To calculate the total number of unique findings in the platform, aggregate the findings across all assets and remove any duplicates.

1. Navigate to the scorecard of a specific company.



2. Click the **Issues** tab.

**SecurityScorecard** | All | Search companies, scorecards, portfolios and tags...

Home | My Organization | Companies | Communication | Automation | Threat Intelligence

**Vulcan Cyber** | vulcan.io · Technology · 27 followers

Create Action Plan or Score Planner | No artifacts shared | Send Request | Actions

**Issues** | 10

Overview | Score Factors | History | **Issues** | Compliance | Incidents | Digital Footprint | Vendor Detection | Hierarchy | Evidence Locker | Company Profile | Risk Quantification

Vulcan Cyber Scorecard > Issues > Open issues

Open | Under Review | Approved | Declined | Decayed

Filter by threat level | Filter by breach risk | Clear Filters | 8 third-party signals | Create Action Plan | Export

Issue	Factor	Threat level	Breach risk	Impact	Findings	Source	Attestation
Count of All systems installed	Application Security	Info	Info	- 0.0	9		
Count of Linux systems installed	Application Security	Info	Info	- 0.0	18		
Count of Mac systems installed	Application Security	Info	Info	- 0.0	7		
Count of Windows systems installed	Application Security	Info	Info	- 0.0	15		
Internal Critical-severity CVE	Application Security	Info	Info	- 0.0	7		

- Review the **Findings** column. Sum the values in this column, but only for rows where the source is SecurityScorecard.

**Important!** Findings from third-party integrations displayed in SecurityScorecard are not imported into Exposure Management.

**SecurityScorecard** | All | Search companies, scorecards, portfolios and tags...

Home | My Organization | Companies | Communication | Automation | Threat Intelligence

Issue	Factor	Threat level	Breach risk	Impact	Findings	Source	Attestation
Network Security	Info	Info	- 0.0	1	SecurityScorecard		
Network Security	Positive	Info	- 0.0	7	SecurityScorecard		
Patching Cadence	Info	Info	- 0.0	1	SecurityScorecard		
Patching Cadence	Info	Info	- 0.0	1	SecurityScorecard		
Patching Cadence	Info	Info	- 0.0	1	SecurityScorecard		
Social Engineering	Info	Info	- 0.0	182	SecurityScorecard		
Application Security	Info	Info	- 0.0	9	SecurityScorecard		
Application Security	Info	Info	- 0.0	18	SecurityScorecard		
Application Security	Info	Info	- 0.0	7	SecurityScorecard		
Application Security	Info	Info	- 0.0	15	SecurityScorecard		
Application Security	Info	Info	- 0.0	7	SecurityScorecard		
Application Security	Info	Info	- 0.0	16	SecurityScorecard		
Application Security	Info	Info	- 0.0	21	SecurityScorecard		
Application Security	Info	Info	- 0.0	6	SecurityScorecard		

In Tenable Exposure Management:



1. [Locate your connector findings](#).
2. Compare the total number of findings between SecurityScorecard and Tenable Exposure Management.

**Expected outcome:** The total number of findings in Exposure Management should match the number of SecurityScorecard-sourced findings shown in the selected asset's scorecard.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.

## SentinelOne Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[SentinelOne](#) provides a range of products and services to protect organizations against cyber threats. The SentinelOne security platform, named [Singularity XDR](#), is designed to protect against various threats, including malware, [ransomware](#), and other advanced persistent threats ([APTs](#)). It uses machine learning and other advanced analytics techniques to analyze real-time security data and identify patterns and behaviors that may indicate a security threat. When a threat is detected, the platform can automatically trigger a response, such as quarantining a device or issuing an alert to security personnel. Our main products are designed to protect the three security surfaces attackers are targeting today: [Endpoint](#), [Cloud](#), and [Identity](#).

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">SentinelOne</a> Endpoint Security <div><b>Note:</b> Cloud and Identity not supported.</div>



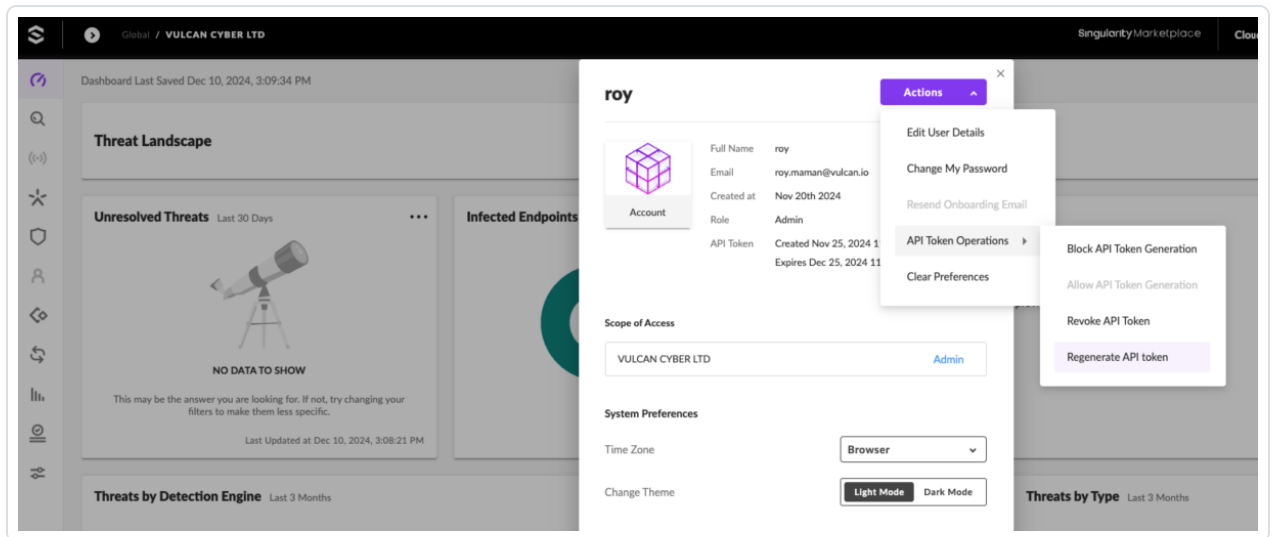
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices Other Resources
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure you have the following:

- Create or use a SentinelOne **Admin** user account.
- Identify your SentinelOne Server URL (e.g., `https://usea1-partners.sentinelone.net`)
- **Generate a SentinelOne API token:**
  1. In the **SentinelOne** platform, navigate to **My User**.
  2. Navigate to **Actions > API Token Operations**.
  3. Click **Generate API tokens**.





4. Enter your Two-Factor Authentication credentials.
5. Save the generated token. You will need it when configuring the connector in Exposure Management.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

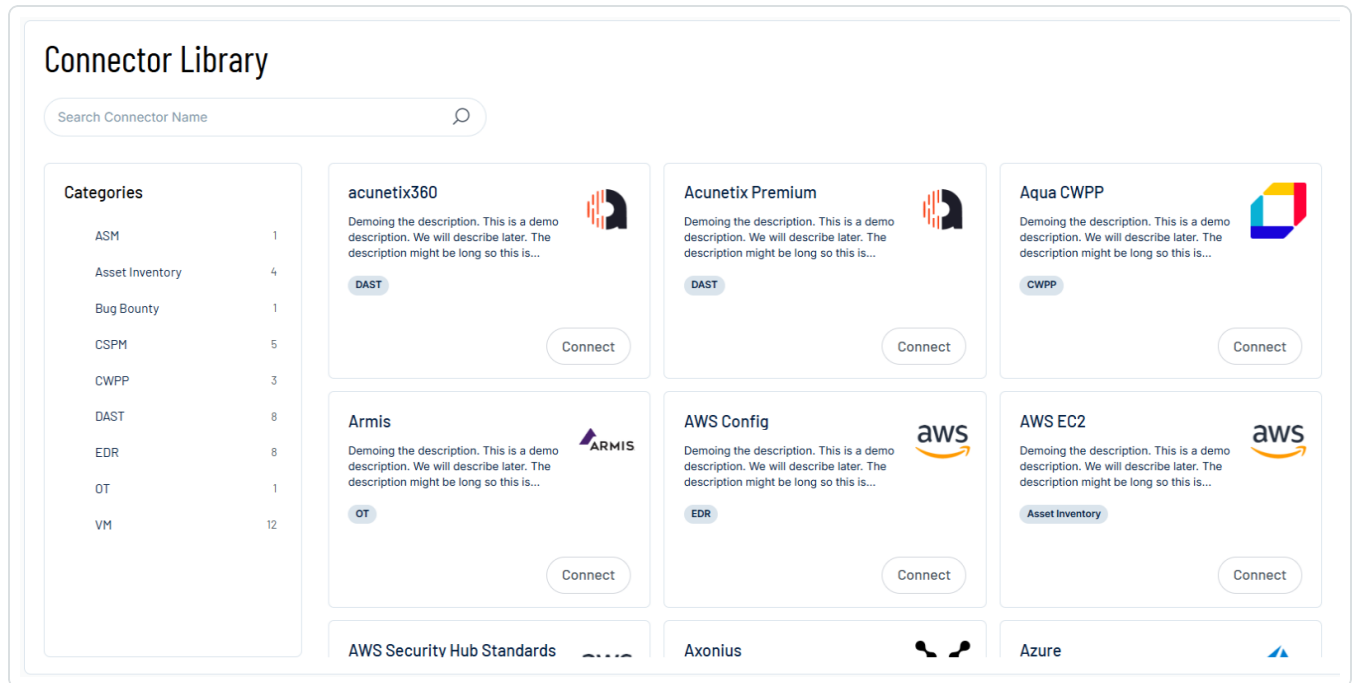
The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	



2. In the upper-right corner, click **+ Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.
4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server URL** and **API Token** text boxes, paste credentials you generated in SentinelOne.



4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - From the **Asset types to fetch** drop-down, select the asset types you want to fetch for.
  - (Optional) To fetch vulnerabilities detected on the assets, select the **Fetch detected vulnerabilities** check box.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

❌ Failed tests 1 out of 4 integration tests failed

✅ Successful tests 3 out of 4 integration tests succeeded

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).



7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

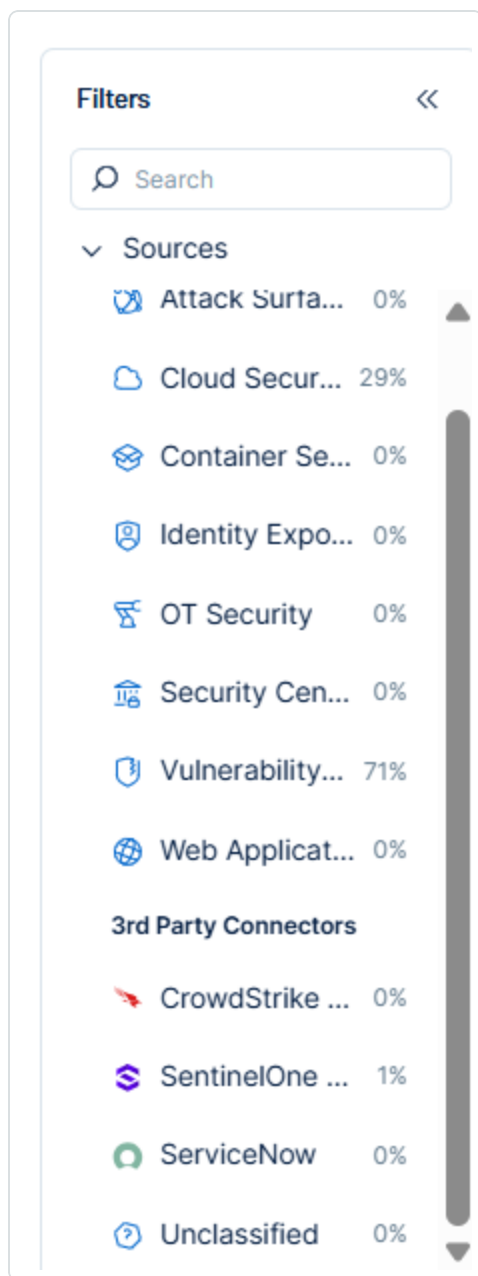
## SentinelOne in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

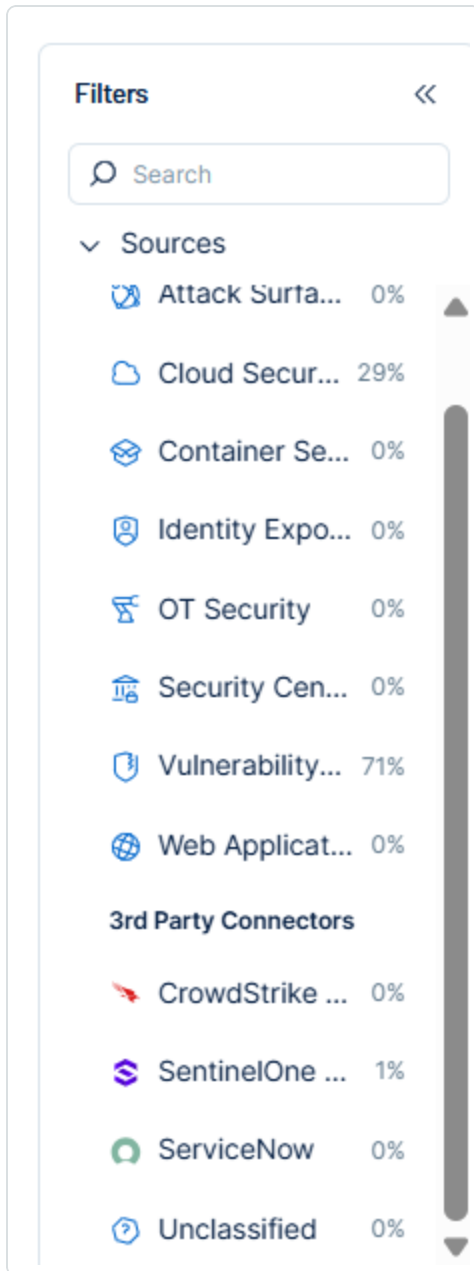
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

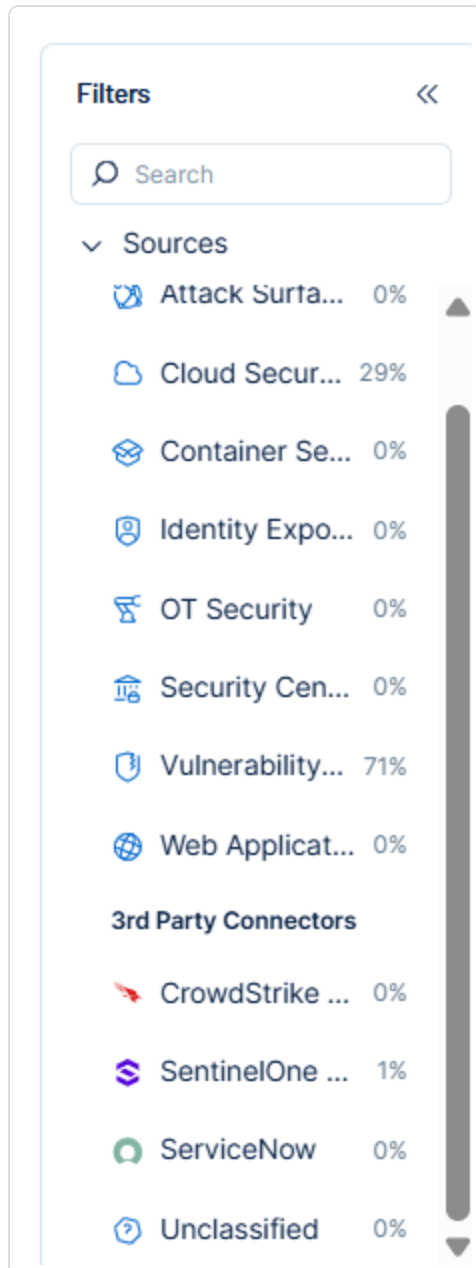
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	SentinelOne Field
Asset Unique Identifier	id
Asset - External Identifier or Asset - Provider Identifier	cloudProviders.<CloudProvider>.cloudInstanceId
Asset - Name	computerName
Other Resources > Cloud Resource Type	machineType
Asset - Operating Systems	osName + osRevision
Asset - IPv4 Adresses Asset - IPv6 Adresses	externalIp
Asset - MAC Addresses	networkInterfaces[*].physical
Asset - First Observation Date	createdAt
Asset - Last Observed At	lastActiveDate
Asset - External Tags	tags
Asset Custom Attributes	machineType siteName groupName





## Finding Mapping

Tenable Exposure Management UI Field	SentinelOne Field
Unique Identifier	cveId + id + endpointId
Finding Name	cveId
CVEs	cveId
Severity Driver	baseScore or severity
Description	description
Finding Custom Attributes	id applicationName applicationVersion publishedDate severity lastScanDate mitreUrl nvdUrl
First Seen	detectionDate
Last seen (Observed)	lastSeenTimestamp

## Finding Status Mapping

Tenable Exposure Management Status	Microsoft TVM Status
Active	All other statuses
Fixed	status = 'Removed' severity = 'False Positive'

**Note:**For Microsoft TVM, Exposure Management ingests only active/vulnerable findings.



## Finding Severity Mapping

Tenable Exposure Management Severity	SentinelOne Score
Critical	<b>CVSS:</b> 9.0 - 10.0 <b>Severity:</b> Critical
High	<b>CVSS:</b> 7.0 - 8.9 <b>Severity:</b> High
Medium	<b>CVSS:</b> 4.0 - 6.9 <b>Severity:</b> Medium
Low	<b>CVSS:</b> 1-3.9 <b>Severity:</b> Low
None	<b>CVSS:</b> 0 <b>Severity:</b> empty

**Note:** For SentinelOne, Tenable uses the `baseScore` or `severity` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>- Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>- Asset not seen for X days according to <b>Last Seen</b>. See <a href="#">Asset Retention</a>.</li></ul>



Change of a Finding status from "Active" to "Fixed"

- Finding no longer appears in the scan findings
- Finding status changes to **Removed**, or **False Positive** on the vendor's side.

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	id
Detection	cveId
Finding	cveId + id + endpointId

## API Endpoints in Use

API version: 2.0

API	Use in Tenable Exposure Management
{{baseUrl}}/web/api/v2.1/agents	Assets
{{baseUrl}}/web/api/v2.1/application-management/risks	Findings, Detections
{{baseUrl}}/web/api/v2.1/application-management/risks/cves	Detections enrichment



## Support and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integrating the Tenable Exposure Management and SentinelOne. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

- The integration supports only API tokens generated for users with a single-scope account.
- If the API token belongs to a user with access to multiple scope accounts, the sync will fail.

## Data Validation

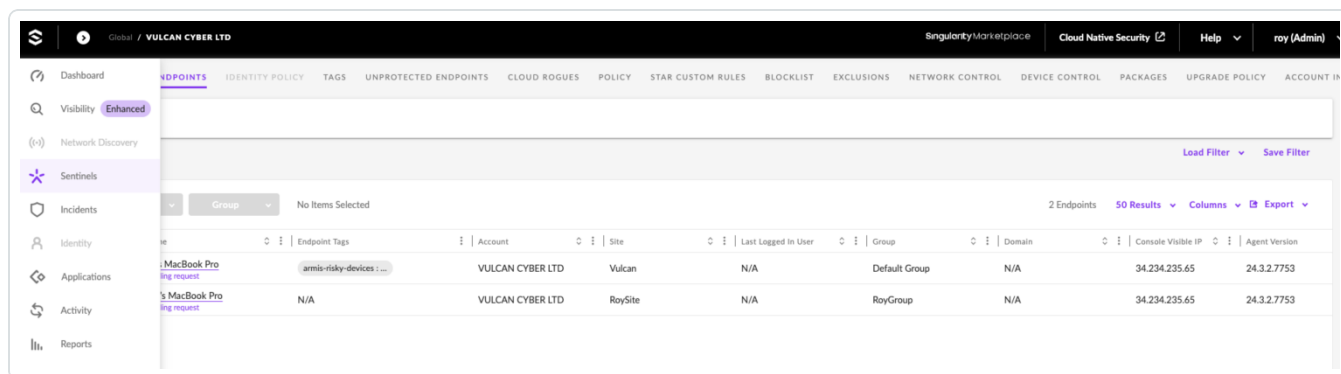
This section shows how to validate and compare data between Tenable Exposure Management and the SentinelOne platform.

### Asset Data Validation

**Objective:** Ensure the number of endpoints (assets) in SentinelOne aligns with the assets displayed in Tenable Exposure Management.

In SentinelOne:

1. Navigate to the **Sentinels** section to view all endpoints. These endpoints represent the assets that should be ingested into Exposure Management.



2. Note the total number of endpoints. If needed, apply filters or use the export option to generate a refined list.

In Tenable Exposure Management:



1. [Locate your connector assets.](#)
2. Compare the number of assets in Tenable Exposure Management to the number of endpoints in SentinelOne.

If an asset is not visible in Exposure Management, check the following conditions:

- Archived based on the last observed date (last seen).
- The asset status changed to one of the selected statuses defined in the [Asset Retention configuration](#).

**Tip:** To learn more on how assets and findings change status, see [Status Update Mechanisms](#).

## Findings Data Validation

**Objective:** Ensure that the total number of findings between SentinelOne and Exposure Management is consistent.

In SentinelOne:

1. Navigate to the **Applications** section and select a specific application from the list.
2. Each application displays its associated endpoint and related CVEs. The combination of these endpoints and CVEs represents the total findings in SentinelOne.

The screenshot shows the SentinelOne Application Management interface. The top navigation bar includes 'Global / VULCAN CYBER LTD', 'SingularityMarketplace', 'Cloud Native Security', 'Help', and 'roy (Admin)'. The main section is titled 'APPLICATION MANAGEMENT' with tabs for 'RISKS', 'INVENTORY', and 'POLICY'. Below this, a filter bar shows 'Safari 16.5.2', 'Vendor: Apple Inc.', 'First Detected: Nov 20, 2024', 'Highest NVD Base Score: 9.8', and 'Severity: Critical'. There are buttons for 'Endpoints (1)' and 'CVEs'. A 'Select filters...' dropdown is present. Below the filters, there is a table of CVEs. The table has columns for CVE ID, Severity, NVD Base Score, Published Date, and Description. The table shows 61 items, with 50 results displayed. The table is sorted by Severity (Critical, High) and NVD Base Score (9.8, 9.3, 8.8). The table includes links to MITRE and NVD for each CVE.

CVE ID	Severity	NVD Base Score	Published Date	Description
CVE-2023-40414	Critical	9.8 (CVSS v3.1)	Sep 26, 2023	A vulnerability, which was cla... <a href="#">MITRE</a> <a href="#">NVD</a>
CVE-2024-44206	Critical	9.3 (CVSS v3.1)	Oct 24, 2024	A vulnerability was found in A... <a href="#">MITRE</a> <a href="#">NVD</a>
CVE-2024-44308	High	8.8 (CVSS v3.1)	Nov 20, 2024	A vulnerability classified as cri... <a href="#">MITRE</a> <a href="#">NVD</a>
CVE-2024-27833	High	8.8 (CVSS v3.1)	Jun 11, 2024	A vulnerability was found in A... <a href="#">MITRE</a> <a href="#">NVD</a>
CVE-2024-27820	High	8.8 (CVSS v3.1)	Jun 11, 2024	A vulnerability was found in A... <a href="#">MITRE</a> <a href="#">NVD</a>

In Tenable Exposure Management:



1. [Locate your connector findings.](#)
2. Compare the number of findings in Tenable Exposure Management to the number in SentinelOne.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Status Update Mechanisms](#).

## ServiceNow Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The [ServiceNow CMDB](#) connector is used to create incidents (both automatically and manually) and extract data from the Configuration Management Database (CMDB). This guide provides a comprehensive overview of setting up and utilizing the ServiceNow connector, detailing the prerequisites, authentication methods, optional features, and API usage.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Service Now CMDB</a>
Category	Endpoint Security
Ingested data	Assets only
Ingested <a href="#">Asset</a>	Devices



<a href="#">Classes</a>	Website Applications
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Identify the ServiceNow Instance Name:**

Locate the name of your hosted ServiceNow instance.

Example: If your URL is `https://dev123456.service-now.com/`, then the instance name is dev123456.

- **Create a ServiceNow user with required roles:**

Ensure the user account has the following roles:

- personalize\_dictionary
- itil
- cmdb\_read
- oauth\_user

- **Choose an authentication method and gather credentials:**

Retrieve the required parameters from your ServiceNow account of the relevant Auth you want to use.

- **Basic Auth:** ServiceNow username and Password. Credentials are used for pulling assets. Make sure the [above permissions](#) are enabled for this user.



- **OAuth2**: ServiceNow username and password + Client ID and Client Secret ID. The keys are used to communicate with the ServiceNow API.
- **Azure AD OAuth 2.0**: An Azure Directory Tenant ID and [Scope](#).

**TIP:** For more info, see [Configure OAuth application in Microsoft Azure](#).

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

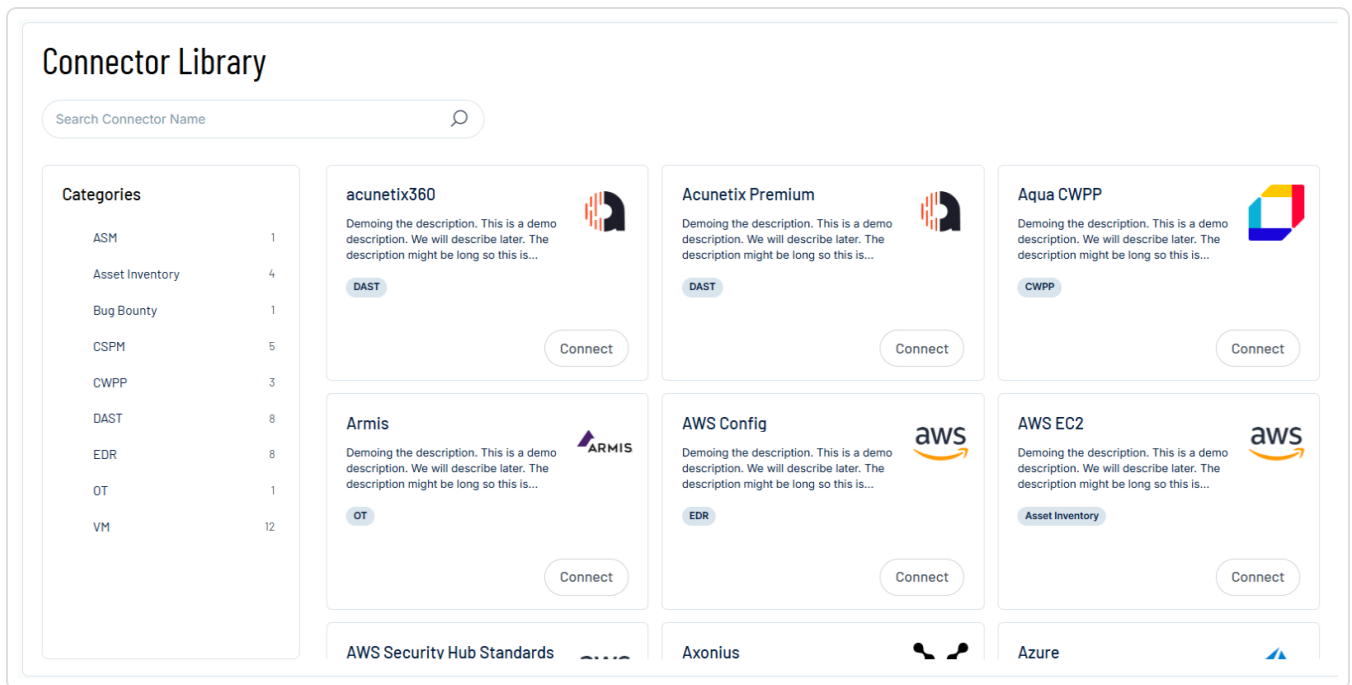
The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.





3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the Instance Name text box, type the name of your ServiceNow instance.
4. From the Authentication Method drop-down, select the method you want to use to authenticate the connector and fill in the relevant auth parameters.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector. Enable the relevant options and configure as needed.



- **Configure ServiceNow CMDB data:** Enable this option so you can customize how data from ServiceNow is mapped into Exposure Management during connector setup:
  - a. On the first screen, choose which ServiceNow tables to include. You can select from the predefined list or specify a custom table.

← Back to ServiceNow

## Configure ServiceNow data

1 ServiceNow tables 2 Tables mapping

### Adding ServiceNow tables

Select the ServiceNow CMDB\_CI tables from which you want to retrieve data into Tenable. A default set of tables is already selected, you can modify or remove them, You can also choose additional tables, including custom ones from your ServiceNow tenant.

Table name

☒ Fetch only parent table assets ⓘ

cmdb\_ci\_computer

cmdb\_ci\_hardware

- b. Select **Next** to proceed to the mapping screen. Here, you can review the default mappings or customize them as needed.
- c. Click Next.

The Mapping screen appears.

- d. Review the default mappings, or customize them as needed.
  - Each asset must have a unique identifier, such as `sys_id` (recommended).
  - All hierarchical tables are expected to include a `sys_class_name` column. This column identifies the record type and enables accurate table inheritance mapping.



**IMPORTANT!** Keep **sys\_id** as the default value for the **asset\_id** field to ensure data integrity. If you select a non-unique field as the **asset\_id**, data may be overwritten between assets that share the same identifier.

- To add an attribute, select the **+** icon on the right.
- To remove an attribute, hover over its name, select the three-dot menu, and choose **Delete**.

**Configure ServiceNow data**

1 ServiceNow tables 2 Tables mapping

Map tables to Tenable's attributes  
Map the data from the selected cmdb\_ci tables into Tenable entities. Define the asset type for each table and map the columns from the ServiceNow tables to the corresponding entity attributes in Tenable. Edits and changes can be made after the initial configuration

Q Search tables...

Table Name	Asset Classes *	Asset ID * ⓘ	Asset Name *	Custom Attributes	IPs	Mac Addresses	Operating System	ⓘ
cmdb_ci.computer	Device	sys_id	name ▼	(assignment_group X) ... ▼	(ip_address X) ▼	(mac_address X) ▼	os ▼	
cmdb_ci.hardware	Device	sys_id	name ▼	(assignment_group X) ... ▼	(ip_address X) ▼	(mac_address X) ▼	Select ▼	

**Note:** Some attributes support mapping multiple fields. Certain attributes apply only to specific asset classes.

- **Collect assets only when their ServiceNow Operational Status is set to '1':** Filters ingested assets to include only those where `operational_status = 1`.
- **Immediately remove assets when their `install_status` matches any of the selected values.**
- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.



- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

**Successful tests** 3 out of 4 integration tests succeeded

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## ServiceNow in Tenable Exposure Management

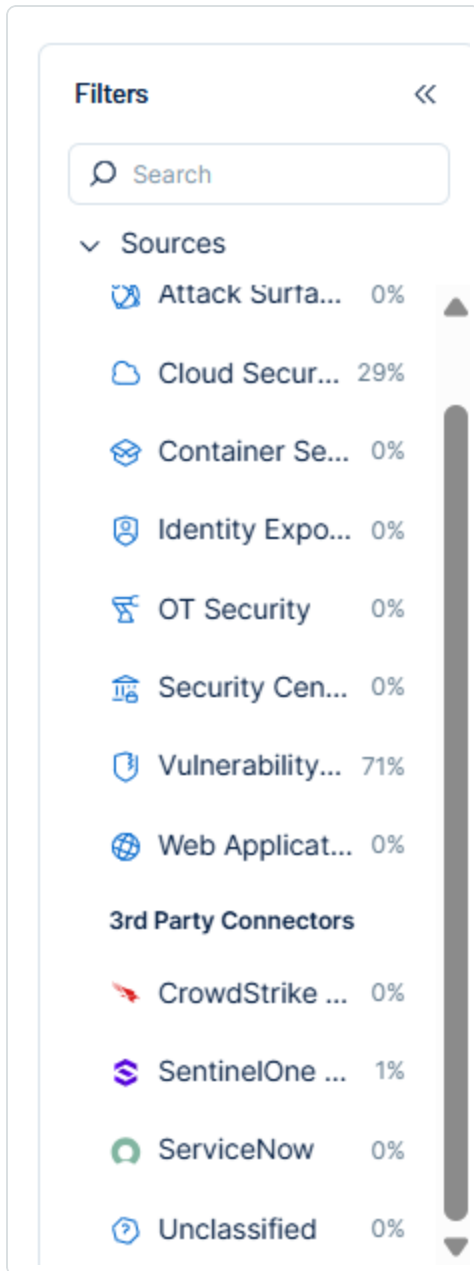
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

## Status Update Mechanisms



Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li><li>Asset status changes to one of the selected statuses defined in the <a href="#">Asset Retention</a> configuration.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#)

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	sys_id

## API Endpoints in Use

API version: 2.0

API	Use in Tenable	Required
-----	----------------	----------



	Exposure Management	Permissions
https://{{{ instance_name }}}.service-now.com/oauth_token.do	Authenticate using OAuth2.	oauth_user
https://{{{ instance_name }}}.service-now.com/api/now/table/	<ul style="list-style-type: none"><li>• Display the specific tables to the user in the UI</li><li>• Fetch the records of the selected table</li></ul>	itil
https://{{{instance_name}}}.service-now.com/api/now/doc/table/schema/	<ul style="list-style-type: none"><li>• Provide the user with the structure of the table columns</li><li>• Identify which column is sys_class_name</li></ul>	personalize_dictionary
https://{{{ instance_name }}}.service-now.com/api/now/table/sys_db_object	Display all tables exist to the user in the UI	<ul style="list-style-type: none"><li>• itil</li><li>• personalize_dictionary</li><li>• not ACL restrict</li></ul>
https://{{{ instance_name }}}.service-now.com/api/now/table/sys_dictionary	Provide the user with the structure of the table columns in one API call	<ul style="list-style-type: none"><li>• itil</li><li>• personalize_dictionary</li><li>• not ACL restrict</li></ul>

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.



## Unique Identifier Requirement

Each asset is expected to include a unique identifier, such as `sys_id`. We strongly recommend using `sys_id` as the default `asset_id`. Using a non-unique field may result in data conflicts, including overwriting data for assets that share the same identifier.

## Hierarchical Table Structure

Each hierarchical table is expected to include a **`sys_class_name`** column. This column is used to distinguish parent assets from child records during ingestion.

### Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the ServiceNow platform.

### Asset Data Validation

**Objective:** Ensure the number of assets/devices in ServiceNow aligns with the number of devices displayed in Tenable Exposure Management.

In ServiceNow:





1. Navigate to **All > System Definition > Tables**.

 tables

Protected Table Log

✓ System Archiving

✓ Archive **Tables**

Archive Knowledge Use

Archive Audit Result

✓ System Clone

✓ Clone Definition

Exclude **Tables**

✓ System Definition

**Tables**

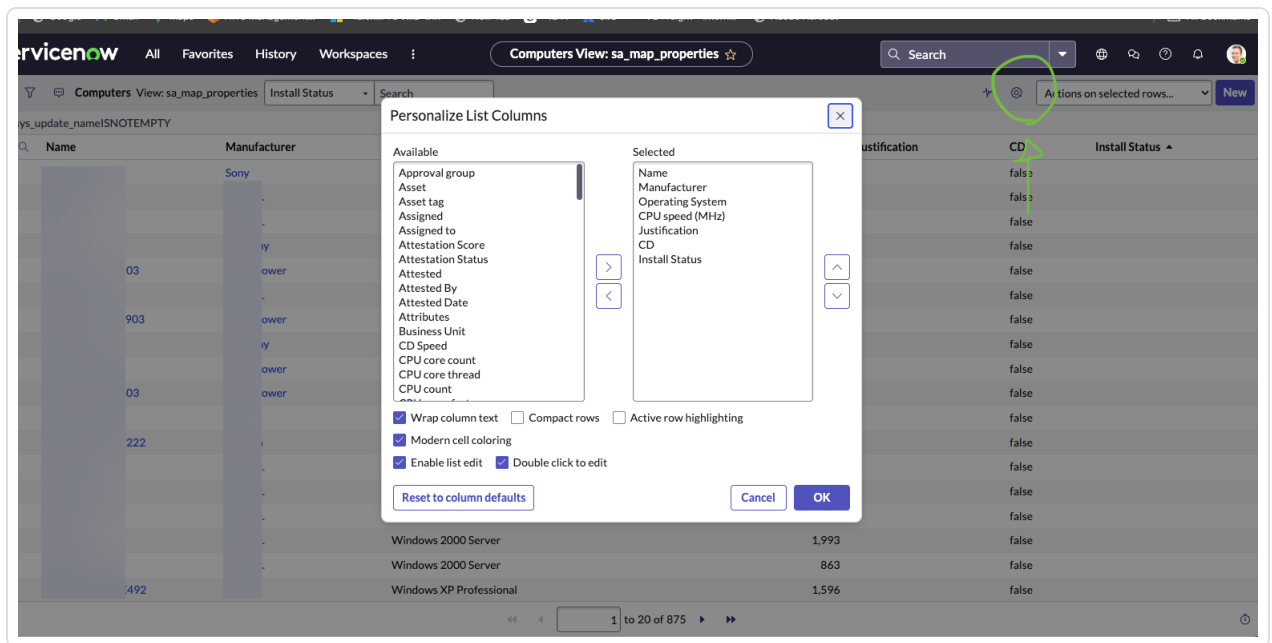
**Tables & Columns**

Decision **Tables**

✓ Remote **Tables**



2. Use the **Label** column to search for the table's user-friendly name, or use the **Name** column to locate the system name used in the integration.
3. Click the relevant table (for example, `cmdb_ci_computer`) to open the list of records.
4. Click the gear icon in the top-right corner to configure the view and add the columns used for filtering. These typically include:
  - `install_status`
  - `sys_class_name` (displayed as **Class**)
  - `operational_status`



5. Click the funnel icon in the top-left corner to apply filters that align with the connector configuration in Exposure Management. For example:
  - `install_status = 1`
  - `operational_status = 1`
  - A specific `sys_class_name`

After applying filters, note the total number of records displayed. This number should align with the devices count shown on the **Devices** page in Tenable Exposure Management.



**IMPORTANT!** The `sys_id` field is used as the unique identifier for ServiceNow assets. If a non-unique field is selected in the connector configuration, discrepancies such as duplicate or overwritten assets may occur.

In Tenable Exposure Management:

1. [Locate your connector assets.](#)
2. Compare the total number of assets between ServiceNow and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in ServiceNow and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- Asset archived because its status changed to one of the selected statuses defined in the [Asset Retention](#) configuration.
- Verify that the asset's `sys_class_name` matches one of the table classes selected in the connector configuration.
- Records that do not contain required fields, such as `sys_id`, may be excluded from ingestion.
- Assets archived based on the value in the `last_seen` column (or an equivalent timestamp field configured in the connector). Only assets considered active at the time of sync are retained.



## Last Seen

Select



Search

attested\_date

checked\_out

delivery\_date

assigned

last\_discovered

**Tip:** To learn more on how assets are archived and findings change status, see [ServiceNow Connector](#).



The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Tanium](#) provides a powerful and flexible platform to secure endpoint devices. Rapidly respond to cyber threats with real-time visibility and comprehensive control.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Tanium</a>
Category	Endpoint Security
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Devices
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Install [Comply - CVE Findings Sensor](#).
- Identify your Tanium client [API Server URL](#) (e.g., `<customerURL>-api.cloud.tanium.com`)
- Create a Tanium User with **API Gateway Permissions** to enable access to the `endpointComplianceFindings` in the GraphQL API.
- Generate a Tanium [API Token](#).



**Note:** When creating the API Token, set the "**Trusted IP**" to 0.0.0.0/0 or an exact IPv4. [Read more here.](#)

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

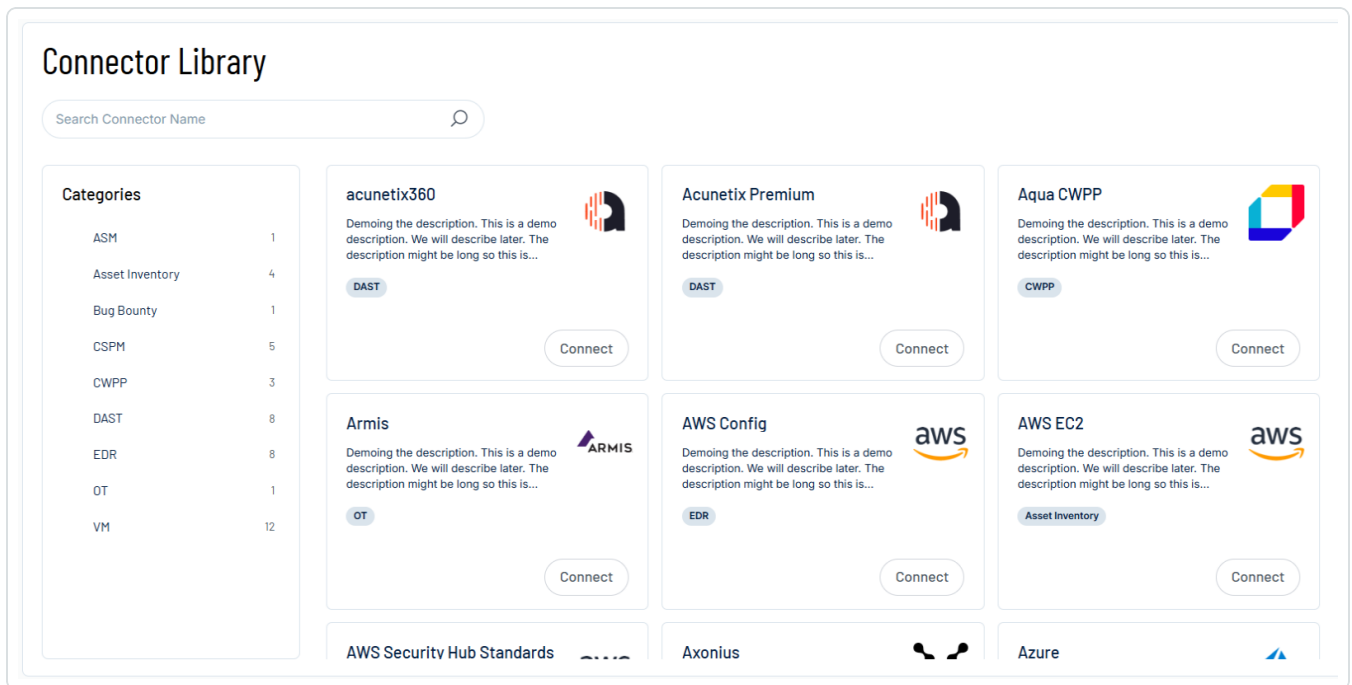
Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on		
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	<div></div>

2. In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Tanium Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server URL** and **Access Token** text boxes, paste the secret credentials you generated in Tanium.
4. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.





- In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

5. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.

- A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

Show tests ▾

**Successful tests** 3 out of 4 integration tests succeeded

Show tests ▾

6. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

7. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
8. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.



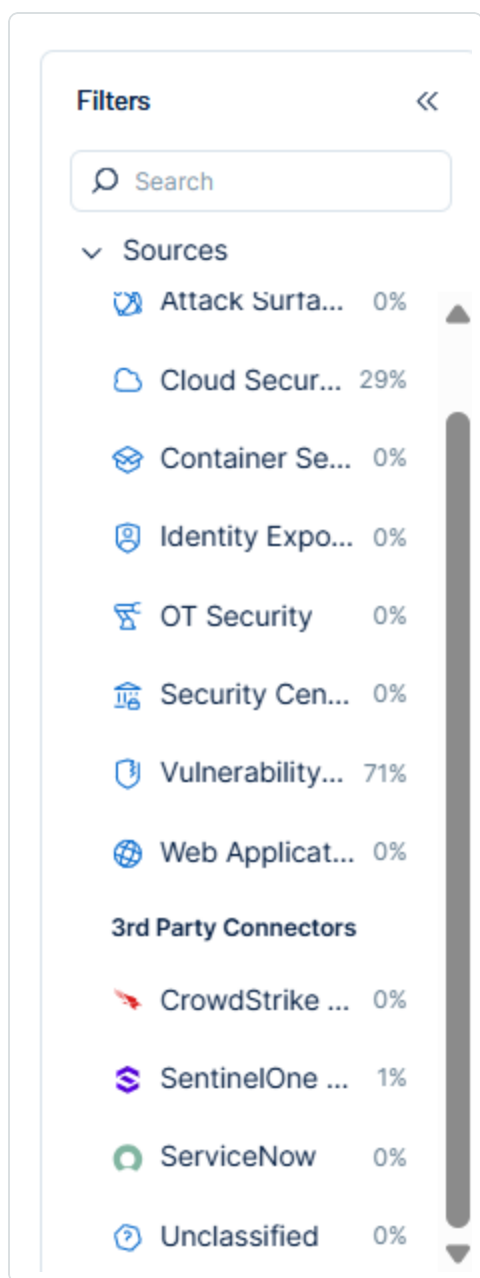
## Tanium in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

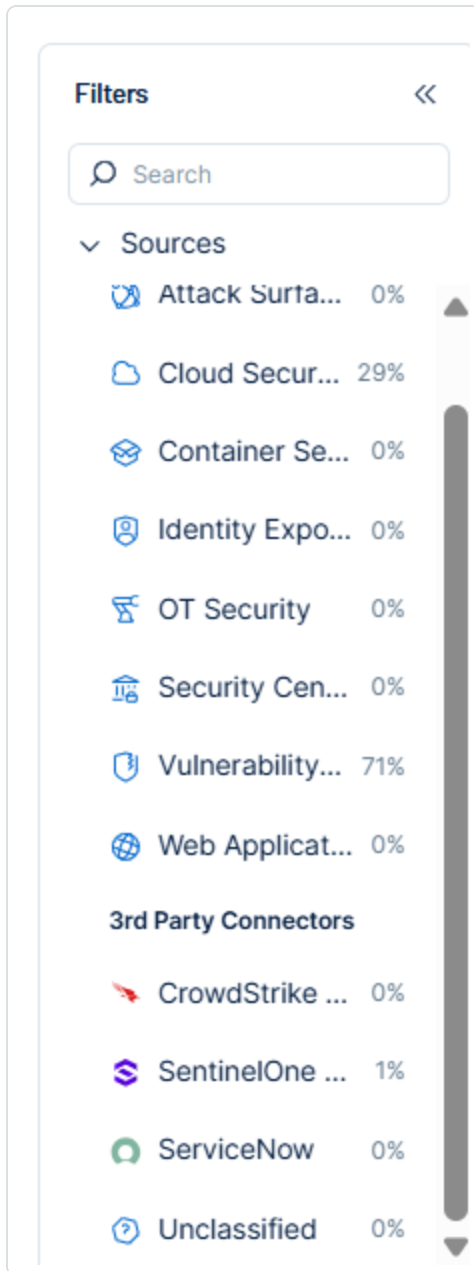
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

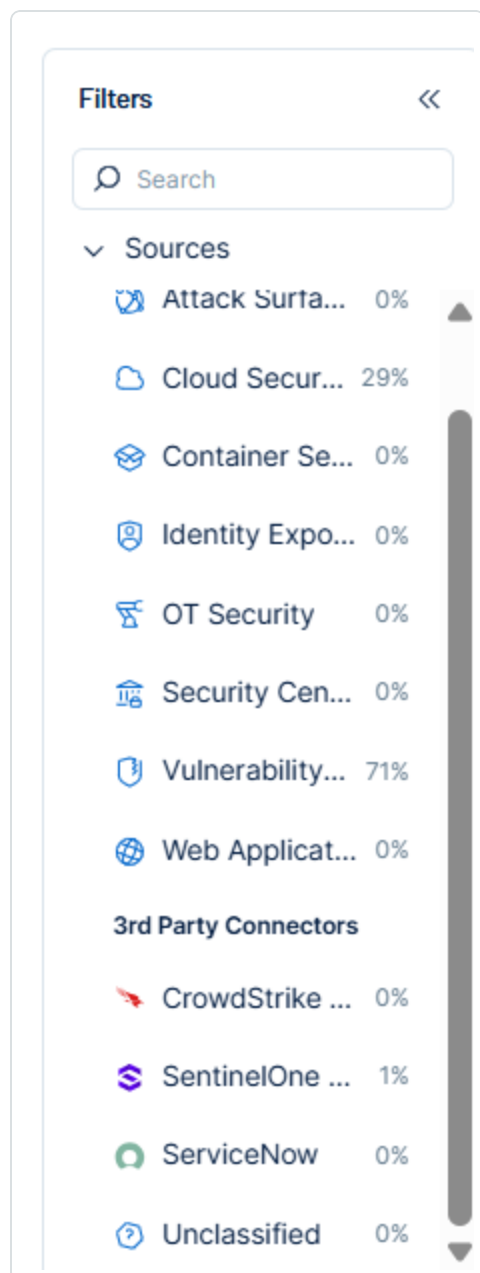
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping

Tenable Exposure Management UI Field	Tanium Field
Unique Identifier	<code>node.id</code>
Asset - Name	<code>node.name</code>
Asset - Operating Systems	<code>node.os.platform</code>
Asset - IPv4 Adresses Asset - IPv6 Adresses	<code>node.ipAddresses</code>
Asset _MAC Addresses	<code>node.macAddresses</code>
Asset - First Observation Date	<code>node.eidFirstSeen</code>
Asset - External Tags	<code>node.sensorReadings.columns</code> <code>node.computerID</code> <code>node.systemUUID</code> <code>node.namespace</code> <code>node.isVirtual</code> <code>node.isEncrypted</code> <code>node.chassisType</code> <code>node.primaryUser.name</code>
Asset Custom Attributes	<code>node.os.generation</code>



## Finding Mapping

Tenable Exposure Management UI Field	Tanium Field
Unique Identifier	cveId + asset_id
Finding Name	cveId
CVEs	cveId
Severity Driver	cvssScoreV3 or cvssScore
Description	summary
Finding Custom Attributes	cveYear Severity SeverityV3

## Finding Status Mapping

Tenable Exposure Management Status	Tanium Status
Active	All fetched findings
Fixed	Findings isn't fetched again during the next sync

## Finding Severity Mapping

Tenable Exposure Management Severity	Tanium Score
Critical	<b>CVSS:</b> 9.0 - 10.0
High	<b>CVSS:</b> 7.0 - 8.9
Medium	<b>CVSS:</b> 4.0 - 6.9
Low	<b>CVSS:</b> 1-3.9
None	<b>CVSS:</b> 0

**Note:**For Tanium, Tenable uses the cvssScoreV3 field to determine severity.



## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	<code>node.id</code>
Detection	<code>cveId</code>
Finding	<code>cveId + cveID + asset_id</code>





## API Endpoints in Use

API	Use in Tenable Exposure Management
{{{ server_url }}}/plugin/products/gateway/graphql	Asset, Detection and Findings

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

The Tanium connector includes an optional checkbox to indicate whether the customer uses the Tanium Comply module.

### Expected Behavior Based on Comply Module Usage

The Tanium connector includes an optional checkbox to indicate whether the Tanium instance uses the **Comply module**.

Comply Module	Checkbox Selected	Expected Behaviour
Yes	Yes	Full synchronization. Assets and findings are retrieved as expected.
No	Yes	Synchronization fails due to query errors. Findings cannot be retrieved.
Yes	No	Synchronization succeeds. Assets and findings are retrieved (same as case 1).
No	No	Synchronization succeeds, but only assets are mapped. Findings are not retrieved.

- If the Comply module is not available and the checkbox is selected, the connector will attempt to run Comply-specific queries, resulting in errors.



- If the Comply module is not available and the checkbox is not selected, the connector will skip findings and sync only assets.

## Tenable On-Prem Connector

The Tenable On-Prem connector requires configuration to establish a connection with Tenable One. This procedure involves the generation of a pairing key within the Tenable One user interface, which is subsequently provided to the gateway during the setup phase. In essence, the Tenable On-Prem connector acts as a secure intermediary, allowing Tenable One to reach into closed networks without compromising their security posture. The key is that the gateway initiates the connection to Tenable One, so no inbound connections to the closed network are required.

### Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Review the *Tenable On-Prem Connector Quick Reference Guide*
- Download the Tenable Core OVA file from the following link:  
<https://www.tenable.com/downloads/tenable-appliance>
- Ensure UDP port 51820 is open and pointing to your region-based server URL.

**Tip:** You can find the region-based server URL on the Add Connector page when you [create the Tenable On-Prem connector](#) within Tenable Exposure Management.

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector



To configure the connector:

1. (Optional) In the **Gateway Name** text box, type a name for the connector.
2. Copy the **Pairing Key** and **UID** values for use within Tenable Core.
3. Finalize the connector configuration within the Tenable Core user interface as described in the [Tenable On-Prem Connector Quick Reference Guide](#).

Upon completion, you can use the connector during the setup of third-party connectors within Tenable Exposure Management.

## Veracode Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Veracode](#) Web Application Scanning combines a DAST assessment tool with static analysis and other technologies to more effectively find, secure, and monitor websites and applications. The tool helps find hidden security issues often missed by other products, looking in directories, debug code, leftover source code, and resource files for information that hackers could exploit to gain access to the application. From hidden usernames and passwords to ODBC connectors and SQL strings, Veracode identifies potential vulnerabilities to enable faster fixes.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Veracode - Dynamic Analysis</a> <b>Note:</b> DAST Essentials is not supported
Category	DAST
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Web Application



Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- **Create or use a Veracode API user with the appropriate permissions:**

A **Reviewer** user with **Results API** role.

For more information, see [Create an API user in the Veracode Platform | Veracode Docs](#).

- **Generate Veracode Credentials (API ID and Secret keys):**

In Veracode:

1. Click on the gear icon and select **Admin**.
2. Navigate to the **Users** tab and click **Add New User**.
3. Type your user details:
  - Provide a descriptive first and last name.
  - Check the **Non-Human User** box.

**IMPORTANT!** You cannot convert an existing user account to an API service account. A new user account must be created with the **Non-Human User** checkbox selected.

4. In **User Settings**, enter a valid email address for the API service account. Veracode will use this address to send notifications regarding error messages, password expiration, and other automated messages.
5. (Optional) [Specify the IP range restrictions for the user](#).



6. In the **User Roles** section, select the APIs the API service account should access (**Results API** role).
7. For the **"Restrict Login IP"** option, select No.
8. Click **Save** to create and enable the user account.

The user will receive an activation email.

**Note:** Before accessing the APIs, users must activate their account, generate API credentials, and [enable HMAC authentication](#).

## Add a Connector

To add a new connector:

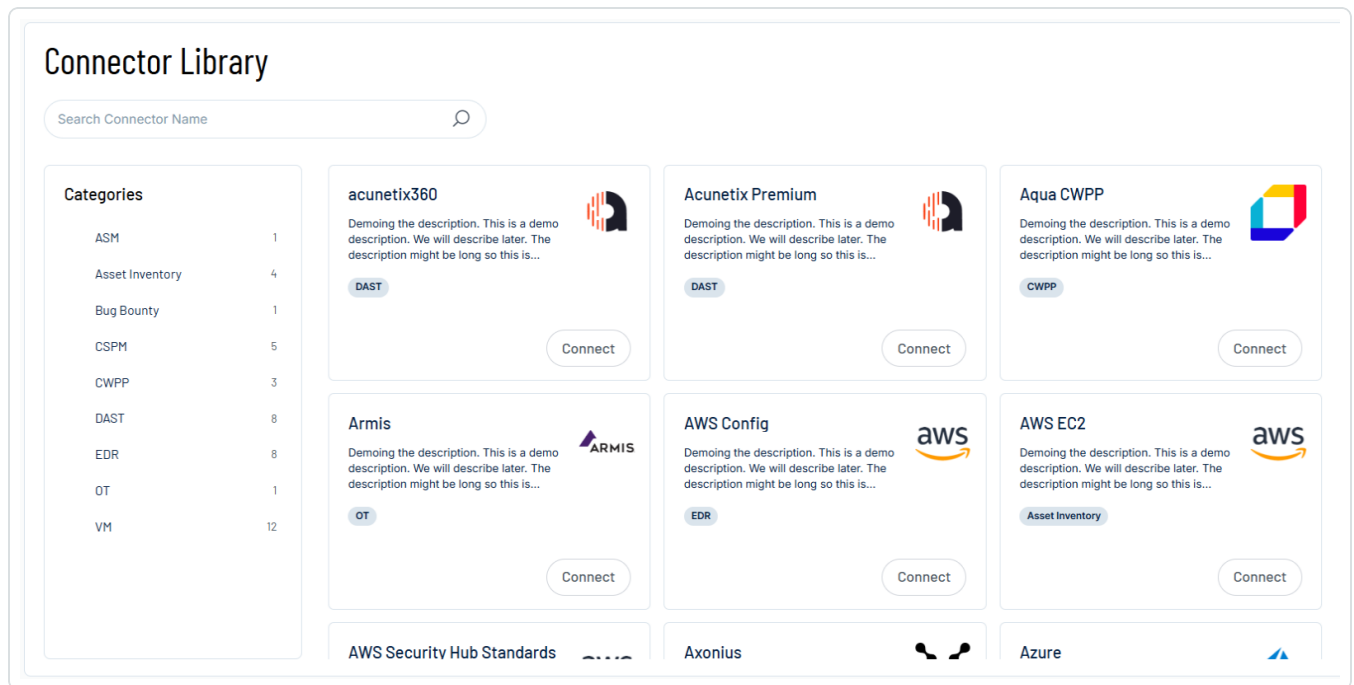
1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.

Connectors						<a href="#">Add new connector</a>
<input type="text" value="Search Connector Name"/>		<input type="text" value="Select"/>				
Name	Connector type	Status	Last data ingestion	Created on		
CrowdStrike111	CrowdStrike	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
NAS 946056	SmallDemoConnector	Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a>	
SecurityScorecard	Security Scorecard	Connected	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a>	
Snyk-guy	Snyk	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Acunetix Premium	Acunetix Premium	Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
Qualys	Qualys	Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a>	
ServiceNow	ServiceNow	Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a>	

2. In the upper-right corner, click **Add new connector**.

The **Connector Library** appears.



3. In the search box, type the name of the connector.

4. On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. From the **Region** drop-down, select the region in which the connector resides, for example, **US**.
4. In the **API Key** and **API Secret** text boxes, paste the client credentials you [generated in Veracode](#).



5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - From the **Veracode findings ingestion** drop-down, select the type of findings you want to fetch from Veracode.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed, as additional syncing or processing issues may arise.
  - If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

**Failed tests** 1 out of 4 integration tests failed

Show tests ▼

**Successful tests** 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:





- Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
- [View the sync logs](#) for the connector to monitor the logs for a successful connection.

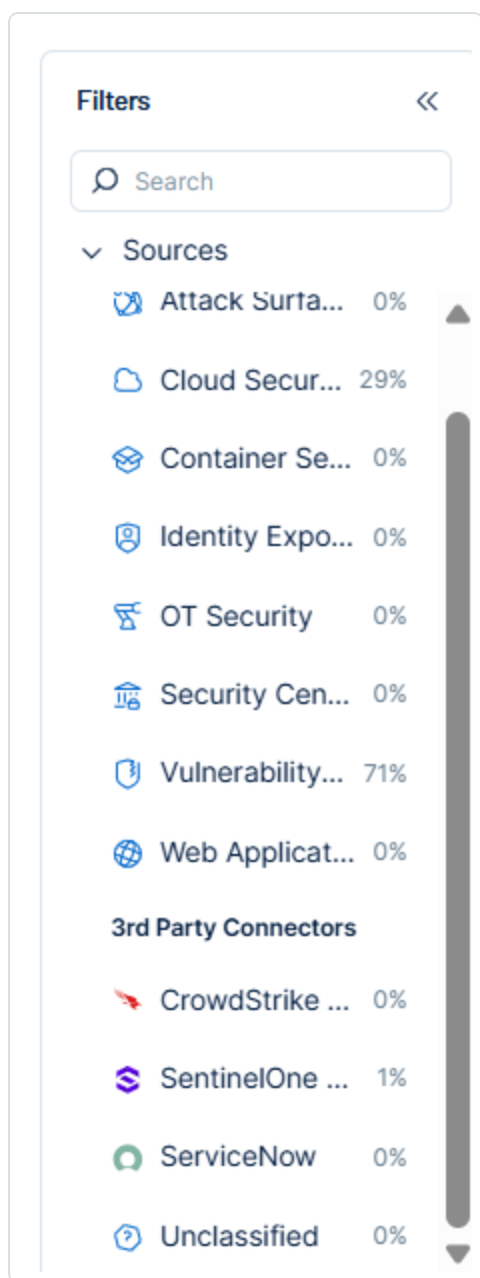
## Veracode in Tenable Exposure Management

### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:

1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

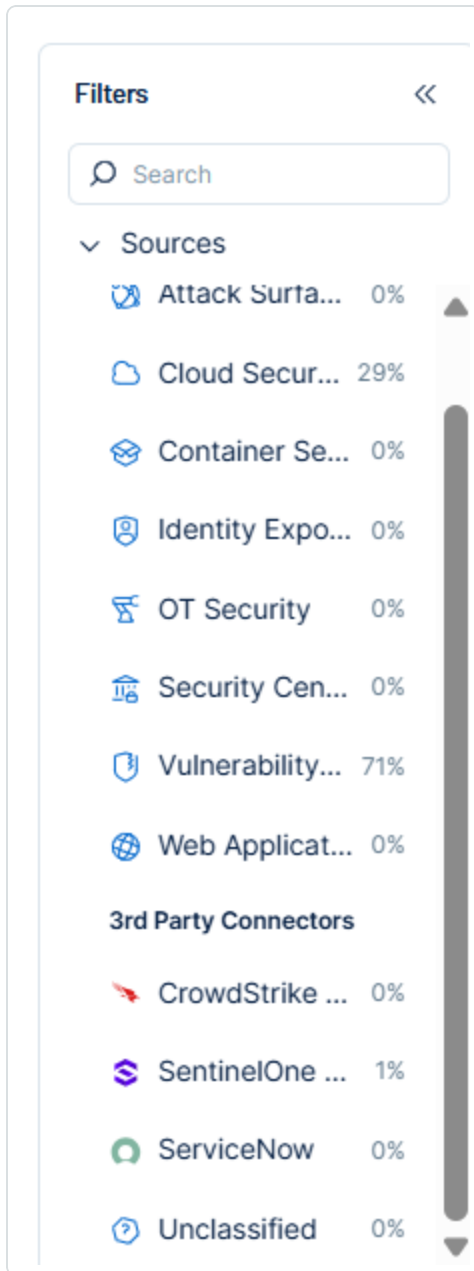
## Locate Connector Weaknesses in Tenable Exposure Management

As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:



1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.



The weaknesses list updates to show only weaknesses from the selected connector.

3. Click on any weakness to view [Weakness Details](#).

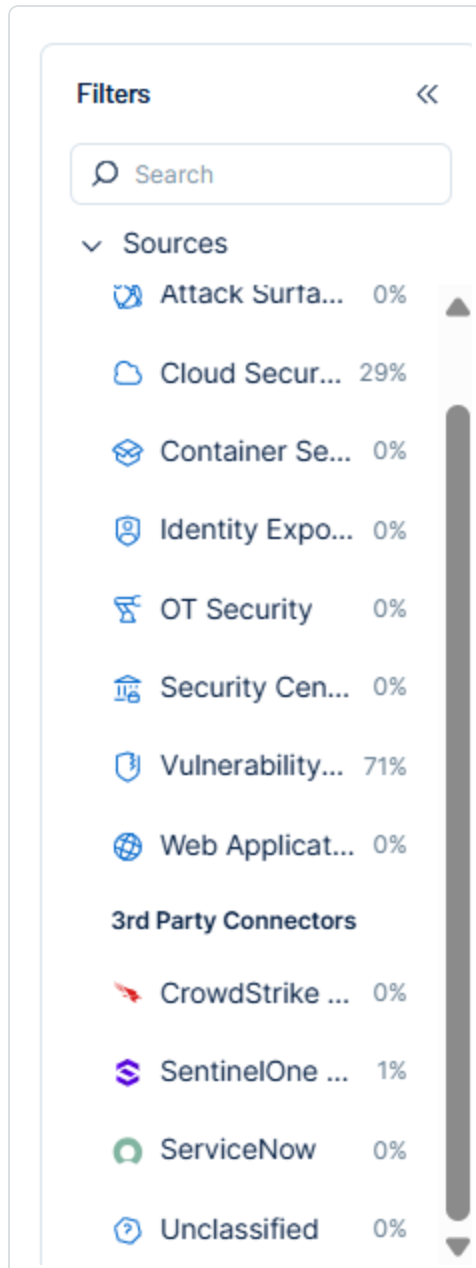
## Locate Connector Findings in Tenable Exposure Management



As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings





The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

**Note:** Veracode applications are mapped into Exposure Management Web Applications, alongside with their detected DAST findings.

## Web Application Mapping

Tenable Exposure Management Value	Veracode Value
Unique Identifier	guid
Asset - Name	profile.name
Asset - First Observation Date	created
Asset - Last Observed At	last_completed_scan_date
Asset - Webapp Homepage Screenshot Url	finding_details.url
Asset - External Tags	profile.tags  Team Name: profile.teams[0].team_name  Business Unit Name: profile.business_unit.name  Business Criticality: profile.business_criticality  custom_fields
Asset Custom Attributes	Business Criticality: profile.business_



	<code>criticality</code>  <code>Policy Compliance Status: profile.policies</code>  <code>Blockcode: profile.custom_fields</code>  <code>IT Director: profile.custom_fields</code>  <code>IT SLT Member: profile.custom_fields</code>  <code>App Profile Url: app_profile_url</code>  <code>Results Url</code>  <code>Id</code>  <code>Guid</code>
--	---

## Finding Mapping

Tenable Exposure Management UI Field	Veracode Field
Unique Identifier	<code>finding_details.finding_category.name + issue_id + application_guid</code>
Finding Name	<code>finding_details.finding_category.name</code>
CVEs	<code>cveId</code>
CWEs	<code>connection_cwes</code>
Severity Driver	<code>finding_details.severity * 2</code>
Description	<code>data.description</code>
Finding Custom Attributes	<code>finding_details.attack_vector</code>  <code>Flaw ID: finding_details.finding_category.id</code>  <code>Vulnerable Parameter: finding_details.vulnerable_parameter</code>  <code>Scan Type: DAST</code>



	<code>Issue Id: issue_id</code> <code>Severity: finding_details.severity</code> <code>Module: finding_details.module</code> <code>Relative Location: finding_details.relative_location</code> <code>Procedure: finding_details.procedure</code> <code>Attack Vector: finding_details.attack_vector</code> <code>File Line Number: finding_details.file_line_number</code> <code>Path: finding_details.path</code> <code>CWE: finding_details.cwe.id</code>
First Seen	<code>finding_status.first_found_date</code>
Last seen (Observed)	<code>finding_status.last_seen_date</code>

### Finding Status Mapping

Tenable Exposure Management Status	Veracode Status
Active	New or Updated
Fixed	Fixed

**Note:**For Veracode, Exposure Management uses the `finding_status.status` field to determine status.

### Finding Severity Mapping

Tenable Exposure Management Severity	Veracode Score
Critical	5
High	4
Medium	2, 3
Low	1



**Note:**For Veracode, Tenable uses the `findings_details.severity * 2` field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding no longer appears in the scan findings</li><li>Finding status changes to <code>close</code> on the vendor's side.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** To learn more about data deduplication and uniqueness criteria, See [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	<code>guid</code>





Detection	<code>finding_details.finding_category.name</code>
Finding	<code>finding_details.finding_category.name + issue_id + application_guid</code>

## Support and Expected Behavior

In Veracode, each application is treated as a single asset of type website. Veracode's API supports fetching both SAST and DAST vulnerabilities; however, there is a distinction in how these vulnerabilities are managed.

**DAST Vulnerabilities:** While Veracode allows scanning additional URLs that are not necessarily linked to applications, the API imposes a limitation—it only supports fetching DAST information when it is explicitly linked to an application.

To link dynamic scans to applications, see [Link Dynamic Analysis results to an application profile | Veracode Docs](#).

Due to the API restriction, Exposure Management only retrieves findings associated with specific applications.

## API Endpoints in Use

API version: v1 , v2

API	Use in Tenable Exposure Management
<code>{{{ region }}}/appsec/v1/applications/</code>	Assets
<code>{{{ region }}}/appsec/v2/applications/{{ application_guid }}/findings</code>	Findings, Detections
<code>{{{ region }}}/appsec/v1/categories/</code>	Enrichment for detections

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Veracode platform.

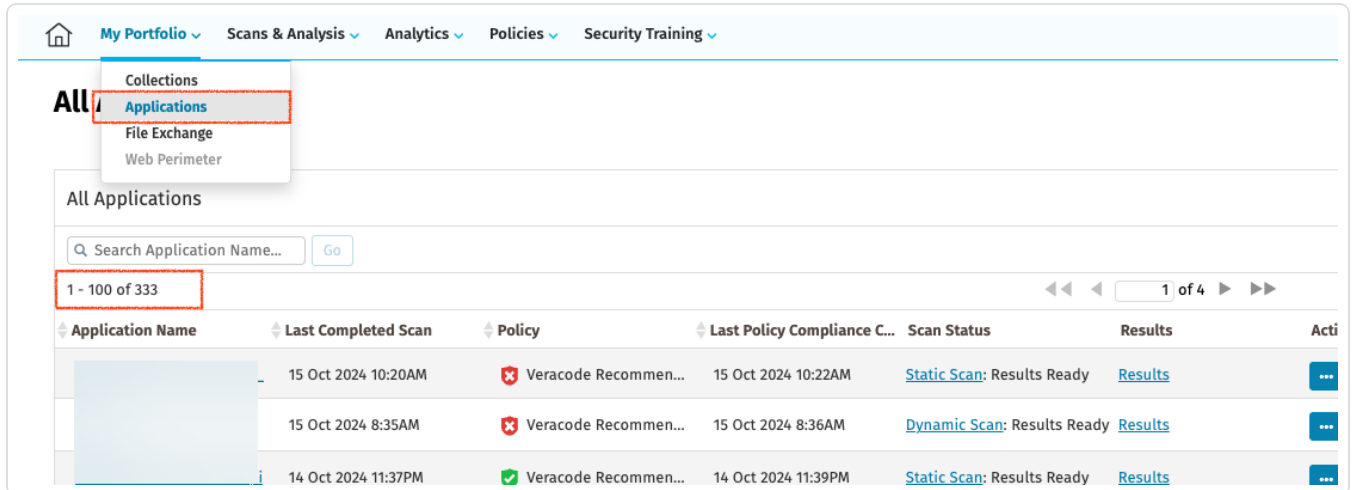
## Asset Data Validation



**Objective:** Ensure the number of endpoints (devices) in Veracode aligns with the number of devices displayed in Tenable Exposure Management. Each application in Veracode is considered a Web Application asset in Exposure Management.

In Veracode:

1. Navigate to **My Portfolio > Applications**.
2. Note the number of applications presented.



In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between Veracode and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Veracode and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset was archived based on its last observed date (`last_completed_scan_date` field).
- The asset was archived because it did not return in the connector's last sync.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

Finding Data Validation

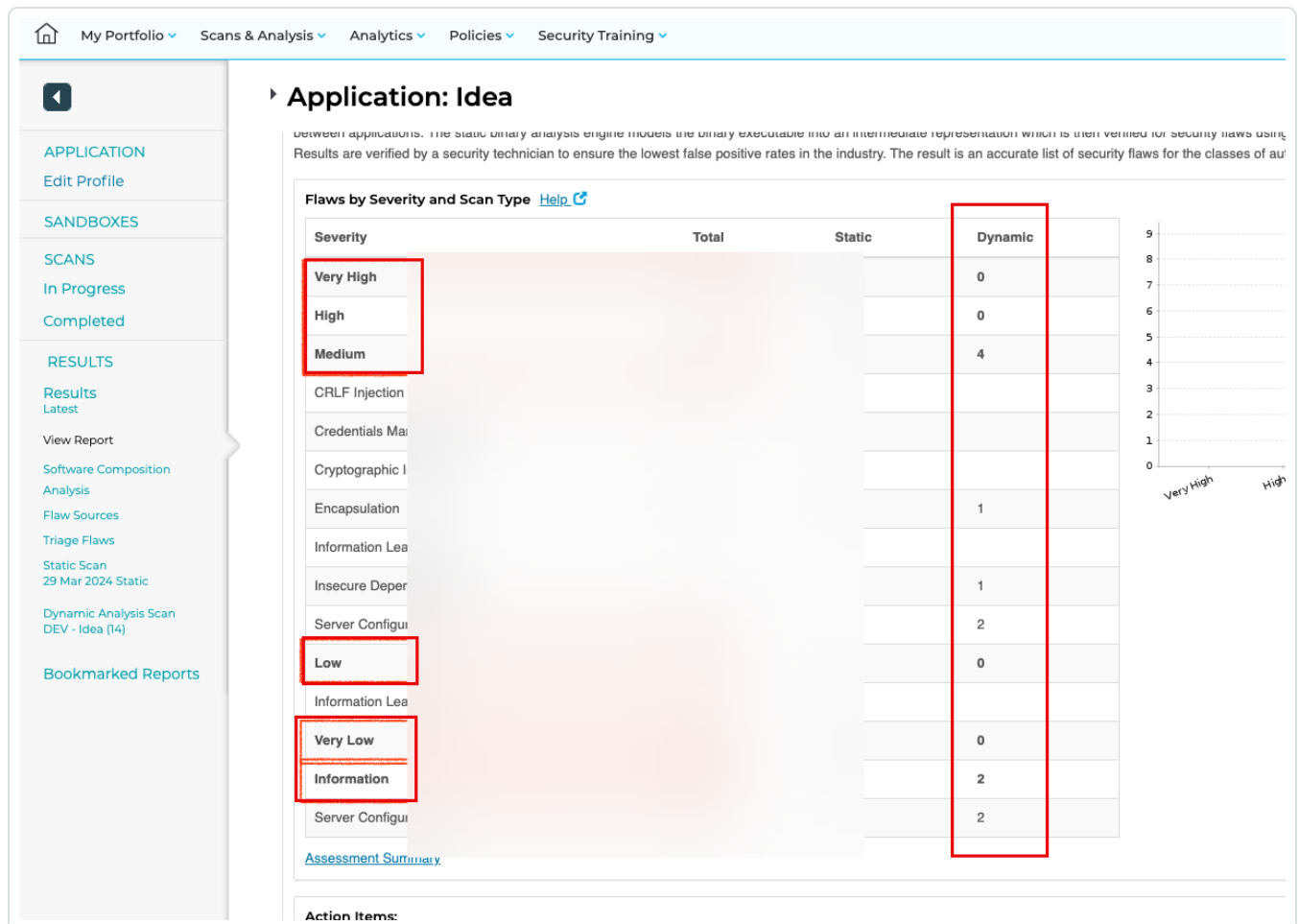


**Objective:** Ensure the number of findings in Veracode aligns with the number of findings in Tenable Exposure Management.

In Veracode:

1. Navigate to **My Portfolio > Applications**.
2. Click on each application from the list, then select **"View Report"** on the left navigation menu.
3. Navigate to the **"Executive Summary"** tab.
4. Summarize the findings listed in the **"Dynamic"** column only for the Very High, High, Medium, Low, Very Low, and Information severities.

Example:



In Tenable Exposure Management:



1. [Locate your connector findings.](#)
2. Compare the total number of findings between Veracode and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Veracode and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets are archived and findings change status, see [Status Update Mechanisms](#).

## Wiz Vulnerabilities Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Wiz](#) scans every layer of cloud environments without agents to provide complete visibility into every technology running in the client's cloud without blind spots. Wiz connects via API to AWS, Azure, GCP, OCI, Alibaba Cloud, VMware vSphere, Openshift, and Kubernetes across virtual machines, containers, and serverless.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Wiz</a>
Category	CWPP
Ingested data	Assets and Findings



Ingested <a href="#">Asset Classes</a>	Device Container Resource Other
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Identify your Wiz API Server URL, e.g. `https://api.example.app.wiz.io`.

- **Have one of the following Wiz Auth URLs:**

- Wiz Commercial: `https://auth.app.wiz.io`
- Wiz for Gov (FedRAMP): `https://auth.app.wiz.us`
- Wiz Commercial hosted on AWS GovCloud: `https://auth.gov.wiz.io`

- **Generate Wiz Client ID and Client Secret:**

For more information, see:

- [Wiz gated documentation portal](#)
- [Wiz prerequisites reference](#)

- **Set the Wiz Service Account:**

1. Sign in to your Wiz instance.
2. Navigate to **Settings > Deployments > Integrations > Vulcan integration**.



**Note:** The integration is still labeled Vulcan in Wiz. Wiz is in the process of updating this label to TenableOne.

3. On the integration page, create a new service account. The required permissions are preconfigured.
4. Click **Create**.
5. Once created, Wiz will display the access key (Client ID) and secret (Client Secret).
6. Copy both values and save them in a secure location.

You'll be required to enter the credentials in the appropriate fields in the connector set up page in Exposure Management.

- **Create or use a user with appropriate access:**

To fetch all projects, the user must have access to all Wiz projects. If you plan to fetch only specific projects, ensure the user has access to those projects.

Policies ▾ Compliance Reports Projects

## New Service Account

**Name**

What's this service account for?

**Type**  
Select which type of software component will use this Service Account

☒ Custom Integration (GraphQL API) ▾

**Projects** optional  
Limit access to selected projects only

Select Projects... ▾

Select up to 5 projects. Leave empty to grant access to all projects

**API Scopes**  
Scopes define the read and write permissions for this account.

☐ All

☐ admin:all      Administrate all admin entities

☐ read:all      Read all entities

☐ update:all      Update all entities

☐ create:all      Create all entities

☐ delete:all      Delete all entities

☐ write:all      Create, update and delete all entities

☐ Audit

Cancel Add

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector





To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server Url** and **Auth Url** text boxes, paste the Wiz server and authentication URLs for your Wiz account.
4. In the **Client ID** and **Client Secret** text boxes, paste the client credentials you generated in Wiz.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Fetch selected Wiz projects** text box, type the Wiz project ID from which you want to fetch data. Leave this box blank if you want to fetch data from all of your available Wiz projects.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) From the drop-down menu, you can choose to automatically remove assets that reach a certain asset status, for example, **Inactive** (selected by default).
6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed,



as additional syncing or processing issues may arise.

- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.



Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ **Failed tests** 1 out of 4 integration tests failed

✖ **Failed tests** 1 out of 4 integration tests failed

✔ **Successful tests** 3 out of 4 integration tests succeeded

✔ **Successful tests** 3 out of 4 integration tests succeeded

[Test connectivity](#)[Show tests](#) [Show tests](#) 

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Wiz Vulnerabilities in Tenable Exposure Management

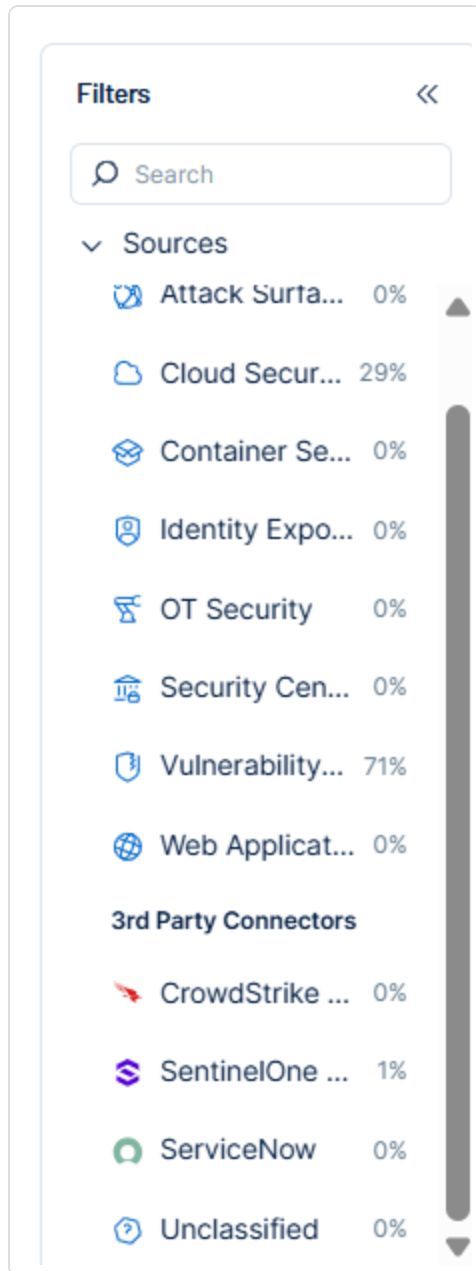
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

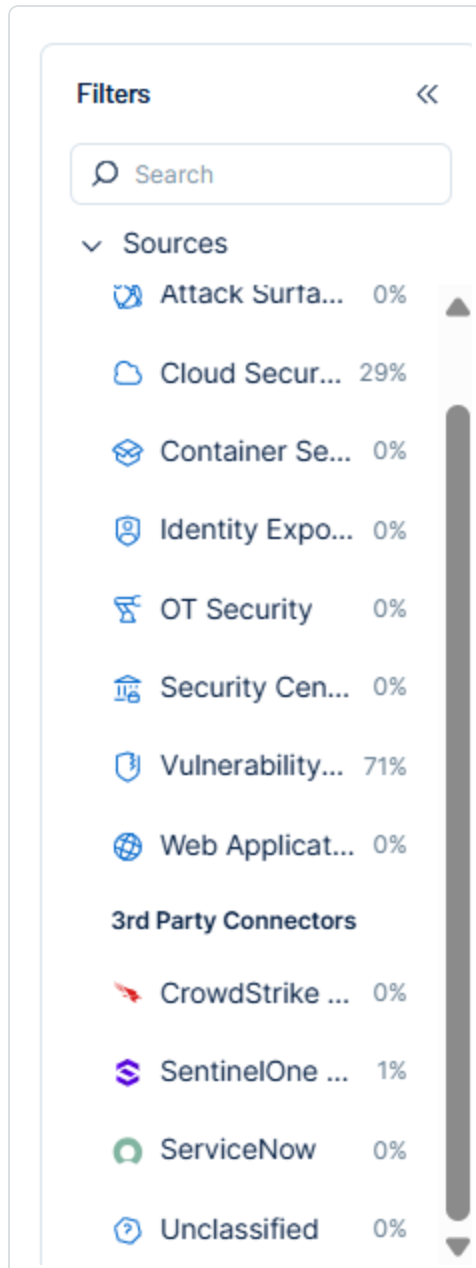
## Locate Connector Weaknesses in Tenable Exposure Management



As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:

1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.





The weaknesses list updates to show only weaknesses from the selected connector.

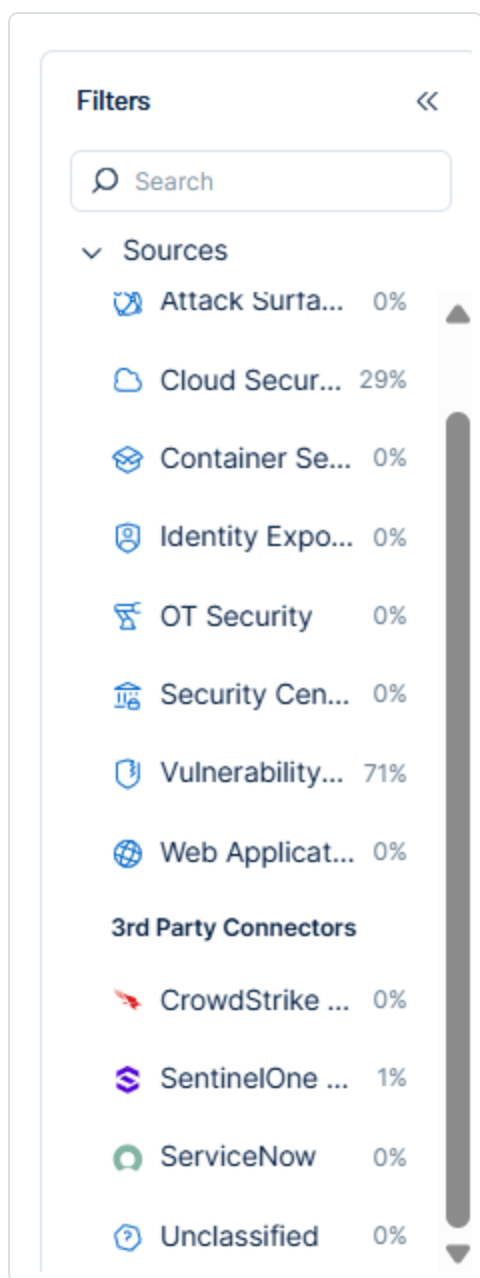
3. Click on any weakness to view [Weakness Details](#).

## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings



The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



Tenable Exposure Management UI Field		WizField
Unique Identifier		Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Asset - External Identifier or Asset - Provider Identifier		Provider ID or External ID
Asset - Name		Name
Asset - Operating Systems		operatingSystem
Asset - IPv4 Adresses Asset - IPv6 Adresses		ipAddresses
Asset - MAC Addresses		network_interfaces.MacAddress
Asset - First Observation Date		creationDate
Asset - Last Observed At		last Seen
Asset - External Tags		Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral



Asset Custom Attributes	os_version
	Projects
	Cloud Platform
	Region
	Subscription
	Subscription ID
	Resource Type
	Native Type
	Provider ID
	External ID
	ImageId
	PublicDnsName
	Role
	FunctionArn
	kind
	cloudProviderURL
	runtime
	status

## Device Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique + Vuln unique+Finding ID
Finding Name	Name
CVEs	Name





Severity Driver	Score
Description	CVEDescription
Finding Custom Attributes	CVSSSeverity FixedVersion Link Finding Type: "Vulnerabilities" DetailedName Version Description ExploitabilityScore ImpactScore HasExploit FindingStatus VendorSeverity LocationPath FixedVersion HasCisaKevExploit DetectionMethod Projects WizURL
First Seen	FirstDetected
Last seen (Observed)	LastDetected

## Container Mapping



Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Asset - Name	Name
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral
Asset Custom Attributes	operatingSystem Images repoExternalId digest Projects Cloud Platform Region



	Subscription
	Subscription ID
	Resource Type
	Native Type
	Provider ID
	External ID
	ImageId
	PublicDnsName
	Role
	FunctionArn
	kind
	cloudProviderURL
	runtime
	status

## Container Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique + Vuln unique+Finding ID
Finding Name	Name
CVEs	Name
Severity Driver	Score
Description	CVEDescription
Finding Custom Attributes	component_id : DetailedName: Version + package_type:DetectionMethod



	CVSSSeverity
	FixedVersion
	Link
	Finding Type: "Vulnerabilities"
	DetailedName
	Version
	Description
	ExploitabilityScore
	ImpactScore
	HasExploit
	FindingStatus
	VendorSeverity
	LocationPath
	FixedVersion
	HasCisaKevExploit
	DetectionMethod
	Projects
	WizURL
First Seen	FirstDetected
Last seen (Observed)	LastDetected

## Other Mapping

Wiz Cloud Resources are mapped to "Other" in the Exposure Management UI.

**Tenable Exposure Management**  
**UI Field**

**Wiz Field**



Unique Identifier	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Asset - Name	Name
Provider Names	Cloud Platform
Cloud Resource Type	Native Type
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral
Asset Custom Attributes	Projects Cloud Platform Region Subscription Subscription ID Resource Type



	Native Type
	Provider ID
	External ID
	ImageId
	PublicDnsName
	Role
	FunctionArn
	kind
	cloudProviderURL
	runtime
	status

## Other Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique + Vuln unique+Finding ID
Finding Name	Name
CVEs	Name
Severity Driver	Score
Description	CVEDescription
Finding Custom Attributes	CVSSSeverity FixedVersion Link Finding Type: "Vulnerabilities" DetailedName



	Version
	Description
	ExploitabilityScore
	ImpactScore
	HasExploit
	FindingStatus
	VendorSeverity
	LocationPath
	FixedVersion
	HasCisaKevExploit
	DetectionMethod
	Projects
	WizURL
First Seen	FirstDetected
Last seen (Observed)	LastDetected

### Finding Status Mapping

Tenable Exposure Management Status	Wiz Status
Active	All other statuses
Fixed	Resolved
	Rejected

**Note:**For Wiz Vulnerabilities, Exposure Management uses the FindingStatus in Full fetch and status in delta fetch.

### Finding Severity Mapping



Tenable Exposure Management Severity	Wiz Score
Critical	<b>CVSS:</b> 9.0 - 10.0
High	<b>CVSS:</b> 7.0 - 8.9
Medium	<b>CVSS:</b> 4.0 - 6.9
Low	<b>CVSS:</b> 1-3.9
None	<b>CVSS:</b> 0

**Note:**For Wiz Vulnerabilities, Tenable uses the Score field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li><li>Asset that returns from the connector with the state "Inactive" (<a href="#">configurable in Data Pulling Configuration</a>)</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding status changes to <b>resolved</b> or <b>rejected</b> on the vendor's side.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria





Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Detection	Name
Finding	Asset unique + Vuln unique + Finding ID
Solution	Remediation

## API Endpoints in Use

API	Use in Tenable Exposure Management	Required Permissions
<code>{{ auth_url }}/oauth/token</code>	Generating OAuth token	None
<code>{{ server_url }}/graphql</code>	Create Inventory and findings reports, Incrementally fetching findings.	<code>create: reports</code> <code>read: reports</code> <code>read: vulnerabilities</code>

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Supported Asset Types

The Wiz connector syncs data only for the following asset types:



- Virtual Machine
- Serverless
- Container
- Container Image

## Asset Identification and Uniqueness

Asset data is retrieved from Wiz Inventory Reports using the Wiz API. These reports do not provide a consistent asset ID field. As a result, the connector uses a combination of other available fields to determine asset uniqueness.

In rare cases, this approach may lead to inaccurate aggregation or unintended deduplication of synced assets.

### Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Wiz Vulnerabilities platform.

**IMPORTANT!** Wiz data is updated frequently, which can make validation challenging. To ensure accurate comparison, include only data that aligns with the last successful sync timestamp, supported asset types, and relevant asset or finding statuses. Applying consistent filters helps maintain validation accuracy. For more info, see [Support and Limitations](#).

### Asset Data Validation

Wiz assets are synced using **Inventory Reports**. For each sync, the connector triggers the Wiz API to generate a report named **Tenable Inventory Report - {{ project\_id }}**. The `project_id` corresponds to the ID provided in the connector configuration. If no ID is provided, `*` is used as the default value.

**Objective:** Ensure the number of assets in **Wiz** aligns with the number of devices displayed in Tenable Exposure Management.

In Wiz:



1. Navigate to the **Reports** section.
2. Locate the generated report titled **Tenable Inventory Report - {{ project\_id }}**.
3. Confirm the relevant timeframe by matching the data to the timestamp of the last successful sync.
4. Filter out unsupported asset types and archived assets in Wiz.  
The Wiz connector only supports the following asset types: **Virtual Machine**, **Serverless**, **Container**, and **Container Image**.
5. Download the report and count the number of rows. Each row represents a single asset.

In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between Wiz and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Wiz and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset's status changed to one of the selected statuses defined in the [Asset Retention](#) configuration (**Inactive** by default).
- Archived based on the last observed date (field **Last Seen**).

**Tip:** To learn more on how assets and findings change status, see [Wiz Vulnerabilities Connector](#).

## Finding Data Validation

Findings data is ingested through Wiz Vulnerabilities Reports. During full syncs, the connector creates reports titled **Tenable Vulnerabilities Report - {{ asset\_type }}**, where **asset\_type** refers to one of the supported asset types listed above.

**Objective:** Ensure the number of findings in Wiz aligns with the number of findings in Tenable Exposure Management.

In Wiz:



1. In the Wiz platform, navigate to the Reports section.
2. Locate the relevant Tenable Vulnerabilities Report - {{ asset\_type }} files for each supported asset type.
3. Download each report and count the number of rows. Each row represents a finding.

**IMPORTANT!** The Wiz connector only supports the following asset types: **Virtual Machine**, **Serverless**, **Container**, and **Container Image**. Make sure to exclude other asset types when validating asset data.

In Tenable Exposure Management:

1. [Locate your connector findings](#).
2. Compare the total number of findings between Wiz Vulnerabilities and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Wiz Vulnerabilities and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Wiz Vulnerabilities Connector](#).

## Wiz Cloud Configurations Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Wiz](#) scans every layer of cloud environments without agents to provide complete visibility into every technology running in the client's cloud without blind spots. Wiz connects via API to AWS, Azure, GCP, OCI, Alibaba Cloud, VMware vSphere, Openshift, and Kubernetes across virtual machines, containers, and serverless.



**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Wiz</a>
Category	CSPM
Ingested data	Assets and Findings
Ingested <a href="#">Asset Classes</a>	Device Container Resource Other
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Identify your Wiz API Server URL (e.g., <https://api.example.app.wiz.io>).
- **Have one of the following Wiz Auth URLs:**
  - Wiz Commercial: <https://auth.app.wiz.io>
  - Wiz for Gov (FedRAMP): <https://auth.app.wiz.us>
  - Wiz Commercial hosted on AWS GovCloud: <https://auth.gov.wiz.io>



- **Generate Wiz Client ID and Client Secret:**

For more information, see:

- [Wiz gated documentation portal](#)
- [Wiz prerequisites reference](#)

- **Set the Wiz Service Account:**

1. Sign in to your Wiz instance.
2. Navigate to **Settings > Deployments > Integrations > Vulcan integration**.

**Note:** The integration is still labeled Vulcan in Wiz. Wiz is in the process of updating this label to TenableOne.

3. On the integration page, create a new service account. The required permissions are preconfigured.
4. Click **Create**.
5. Once created, Wiz will display the access key (Client ID) and secret (Client Secret).
6. Copy both values and save them in a secure location.

You'll be required to enter the credentials in the appropriate fields in the connector set up page in Exposure Management.

- **Create or use a user with appropriate access:**

To fetch all projects, the user must have access to all Wiz projects. If you plan to fetch only specific projects, ensure the user has access to those projects.

Policies ▾ Compliance Reports Projects

## New Service Account

**Name**

What's this service account for?

**Type**  
Select which type of software component will use this Service Account

☒ Custom Integration (GraphQL API) ▾

**Projects** optional  
Limit access to selected projects only

Select Projects... ▾

Select up to 5 projects. Leave empty to grant access to all projects

**API Scopes**  
Scopes define the read and write permissions for this account.

☐ All

☐ admin:all Administrate all admin entities

☐ read:all Read all entities

☐ update:all Update all entities

☐ create:all Create all entities

☐ delete:all Delete all entities

☐ write:all Create, update and delete all entities

☐ Audit

Cancel Add

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.

The **Connectors** page appears.
















Connectors

Search Connector Name

Select

+

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	<a href="#">Show logs</a> <span></span>
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	<a href="#">Show logs</a> <span></span>

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector

- 900 -





To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server Url** and **Auth Url** text boxes, paste the Wiz server and authentication URLs for your Wiz account.
4. In the **Client ID** and **Client Secret** text boxes, paste the client credentials you generated in Wiz.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Fetch selected Wiz projects** text box, type the Wiz project ID from which you want to fetch data. Leave this box blank if you want to fetch data from all of your available Wiz projects.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) From the drop-down menu, you can choose to automatically remove assets that reach a certain asset status, for example, **Inactive** (selected by default).
6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed,



as additional syncing or processing issues may arise.

- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ **Failed tests** 1 out of 4 integration tests failed

✖ **Failed tests** 1 out of 4 integration tests failed

✔ **Successful tests** 3 out of 4 integration tests succeeded

✔ **Successful tests** 3 out of 4 integration tests succeeded

Test connectivity

Show tests ▼

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Wiz Vulnerabilities in Tenable Exposure Management

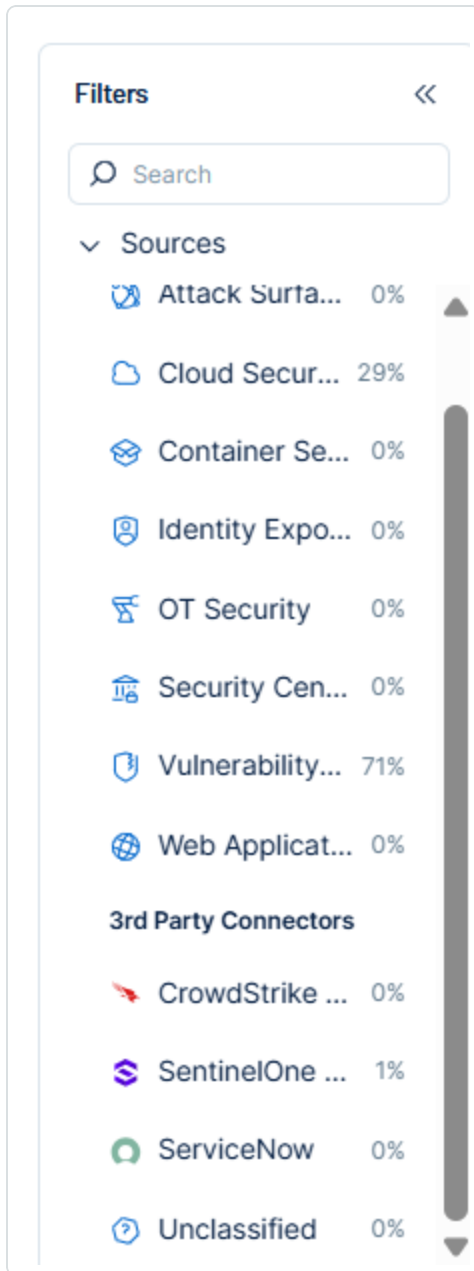
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

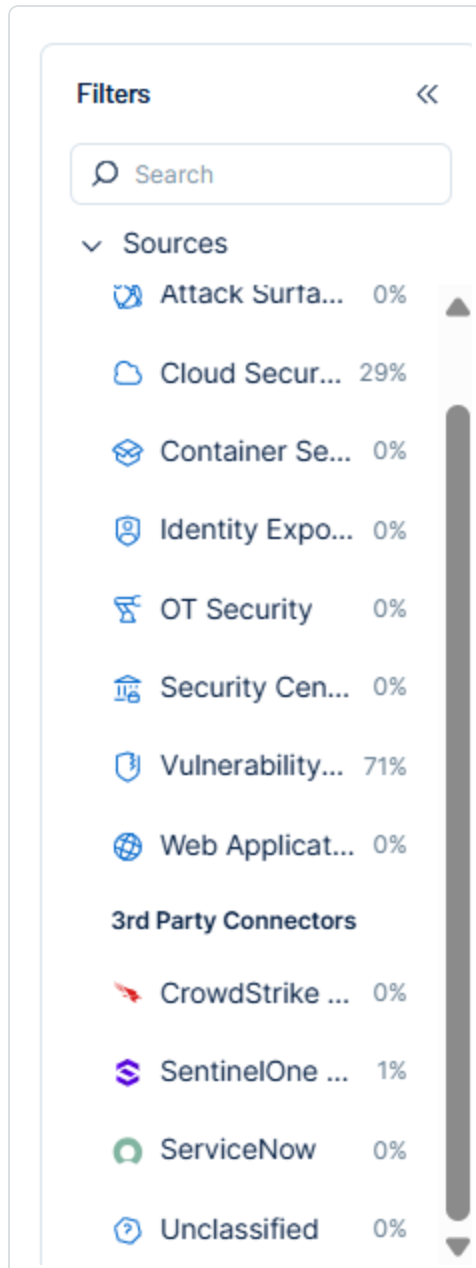
## Locate Connector Weaknesses in Tenable Exposure Management



As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:

1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.





The weaknesses list updates to show only weaknesses from the selected connector.

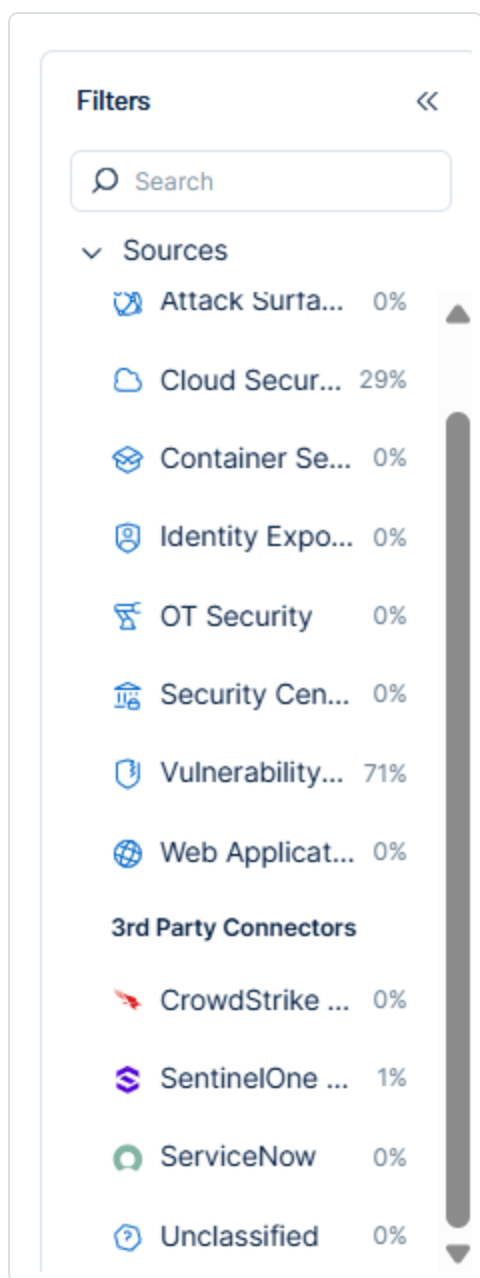
3. Click on any weakness to view [Weakness Details](#).

## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings



The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Name + Provider ID + subscriptionExternalId
Asset - External Identifier or Asset - Provider Identifier	Provider ID or External ID
Asset - Name	Name
Asset - Operating Systems	operatingSystem
Asset - IPv4 Adresses Asset - IPv6 Adresses	ipAddresses
Asset - MAC Addresses	network_interfaces.MacAddress
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral
Asset Custom Attributes	os_version Projects



	Cloud Platform
	Region
	Subscription
	Subscription ID
	Resource Type
	Native Type
	Provider ID
	External ID
	ImageId
	PublicDnsName
	Role
	FunctionArn
	kind
	cloudProviderURL
	runtime
	status

## Device Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique (Name + Provider ID + subscriptionExternalId)+ rule.id + Finding ID
Finding Name	rule.name
Severity Driver	severity
Finding Custom Attributes	Function As Control





	Finding Type:"Configurations" ID Resource External ID Resource Provider Unique ID Resource Deleted Result Status Severity Remediation
First Seen	firstSeenAt
Last seen (Observed)	analyzedAt

## Container Mapping

Wiz Container Images are mapped to Container in the Exposure Management UI.

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Name + Provider ID + subscriptionExternalId
Asset - Name	Name
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription



	<div>Subscription ID</div> <div>image_source</div> <div>Wide Internet Exposure</div> <div>Image Name</div> <div>isPublic</div> <div>isEphemeral</div>
Asset Custom Attributes	<div>operatingSystem</div> <div>Images</div> <div>repoExternalId</div> <div>digest</div> <div>Projects</div> <div>Cloud Platform</div> <div>Region</div> <div>Subscription</div> <div>Subscription ID</div> <div>Resource Type</div> <div>Native Type</div> <div>Provider ID</div> <div>External ID</div> <div>ImageId</div> <div>PublicDnsName</div> <div>Role</div> <div>FunctionArn</div> <div>kind</div>



	cloudProviderURL
	runtime
	status

## Container Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique (Name + Provider ID + subscriptionExternalId)+ rule.id + Finding ID
Finding Name	rule.name
Severity Driver	severity
Finding Custom Attributes	Function As Control Finding Type:"Configurations" ID Resource External ID Resource Provider Unique ID Resource Deleted Result Status Severity Remediation
First Seen	firstSeenAt
Last seen (Observed)	analyzedAt

## Other Mapping

Tenable Exposure Management UI Field	Wiz Field
--------------------------------------	-----------



Unique Identifier	Name + Provider ID + subscriptionExternalId
Asset - Name	Name
Provider Names	Cloud Platform
Cloud Resource Type	Native Type
Asset - External Identifier	Provider ID
Asset - Provider Identifier	
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral
Asset Custom Attributes	Projects Cloud Platform Region Subscription Subscription ID



	Resource Type
	Native Type
	Provider ID
	External ID
	ImageId
	PublicDnsName
	Role
	FunctionArn
	kind
	cloudProviderURL
	runtime
	status

## Other Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique (Name + Provider ID + subscriptionExternalId)+ rule.id + Finding ID
Finding Name	rule.name
Severity Driver	severity
Finding Custom Attributes	Function As Control Finding Type:"Configurations" ID Resource External ID Resource Provider Unique ID



	Resource Deleted Result Status Severity Remediation
First Seen	firstSeenAt
Last seen (Observed)	analyzedAt

### Finding Status Mapping

Tenable Exposure Management Status	Wiz Status
Active	All other statuses
Fixed	Resolved Rejected

**Note:**For Wiz Configurations, Exposure Management uses the `status` field.

### Finding Severity Mapping

Tenable Exposure Management Severity	Wiz Score
Critical	Severity: Critical
High	Severity: High
Medium	Severity: Medium
Low	Severity: Low
None	Severity: Informational

**Note:**For Wiz Configurations, Tenable uses the `Severity` field to determine severity.



## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a>.</li><li>Asset that returns from the connector with the state "Inactive" (<a href="#">configurable in Data Pulling Configuration</a>).</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding status changes to resolved or rejected on the vendor's side.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.

**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	Name + Provider ID + subscriptionExternalId



Detection	<code>rule.id</code>
Finding	Asset unique + Vuln unique + Finding ID

## API Endpoints in Use

API	Use in Tenable Exposure Management	Required Permissions
<code>{{ auth_url }}</code> <code>}}/oauth/token</code>	Generating OAuth token	None
<code>{{ server_url }}</code> <code>}}/graphql</code>	Create Inventory reports, Full and incrementally fetching cloud configurations findings.	<code>create: reports</code> <code>read: reports</code> <code>read: cloud_configuration</code>

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Supported Asset Types

The Wiz connector syncs data only for the following asset types:

- Virtual Machine
- Serverless
- Container
- Container Image

### Asset Identification and Uniqueness

Asset data is retrieved from Wiz Inventory Reports using the Wiz API. These reports do not provide a consistent asset ID field. As a result, the connector uses a combination of other available fields to





determine asset uniqueness.

In rare cases, this approach may lead to inaccurate aggregation or unintended deduplication of synced assets.

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Wiz Vulnerabilities platform.

**IMPORTANT!** Wiz data is updated frequently, which can make validation challenging. To ensure accurate comparison, include only data that aligns with the last successful sync timestamp, supported asset types, and relevant asset or finding statuses. Applying consistent filters helps maintain validation accuracy. For more info, see [Support and Limitations](#).

## Asset Data Validation

Asset data is synced using Inventory Reports via the Wiz API. For each sync, the connector generates a report titled **Tenable Inventory Report**.

**Objective:** Ensure the number of assets in **Wiz** aligns with the number of devices displayed in Tenable Exposure Management.

In Wiz:

1. Navigate to the **Reports** section.
2. Locate the most recent report named **Tenable Inventory Report**.
3. Confirm the relevant timeframe by matching the data to the timestamp of the last successful sync.
4. Filter out unsupported asset types and archived assets in Wiz. The Wiz connector only supports the following asset types: **Virtual Machine**, **Serverless**, **Container**, and **Container Image**.
5. Download the report and count the number of rows. Each row represents a single asset.

In Tenable Exposure Management:



1. [Locate your connector assets.](#)
2. Compare the total number of assets between Wiz and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Wiz and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset's status changed to one of the selected statuses defined in the [Asset Retention](#) configuration (Inactive by default).
- Archived based on the last observed date (field `Last Seen`).

**Tip:** To learn more on how assets and findings change status, see [Wiz Cloud Configurations Connector](#).

## Finding Data Validation

Configuration findings are ingested using the **CloudConfigurationFindingsPage GraphQL** query in Wiz.

**Objective:** Ensure the number of findings in Wiz aligns with the number of findings in Tenable Exposure Management.

In Wiz:

1. Navigate to the **Cloud Configuration Findings** view
2. Filter the results to:
  - Exclude findings related to unsupported asset types.
  - Exclude archived assets.
  - Exclude findings resolved before the first fetch.
  - Match the timestamp of the last successful sync.
3. If the findings are aggregated by rule ID, sum the number of associated resources per rule to determine the total finding count.

In Tenable Exposure Management:



1. [Locate your connector findings.](#)
2. Compare the total number of findings between Wiz and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Wiz and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Wiz Cloud Configurations Connector](#).

## Wiz Issues Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

[Wiz](#) scans every layer of cloud environments without agents to provide complete visibility into every technology running in the client's cloud without blind spots. Wiz connects via API to AWS, Azure, GCP, OCI, Alibaba Cloud, VMware vSphere, Openshift, and Kubernetes across virtual machines, containers, and serverless.

**Tip:** For more information on how third-party integrations work, see [Connectors](#).

## Connector Details

Details	Description
Supported products	<a href="#">Wiz</a>
Category	ASM
Ingested data	Assets and Findings
Ingested <a href="#">Asset</a>	Device



<a href="#">Classes</a>	Container Resource Other
Integration type	UNI directional (data is transferred from the Connector to Tenable Exposure Management in one direction)
Supported version and type	SaaS (latest)

## Prerequisites and User Permissions

Before you begin configuring the connector, make sure to:

- Wiz API Server URL, e.g. `https://api.example.app.wiz.io`.
- **Have one of the following Wiz Auth URLs:**
  - Wiz Commercial: `https://auth.app.wiz.io`
  - Wiz for Gov (FedRAMP): `https://auth.app.wiz.us`
  - Wiz Commercial hosted on AWS GovCloud: `https://auth.gov.wiz.io`

- **Generate Wiz Client ID and Client Secret:**

For more information, see:

- [Wiz gated documentation portal](#)
- [Wiz prerequisites reference](#)

- **Set the Wiz Service Account:**

1. Sign in to your Wiz instance.
2. Navigate to **Settings > Deployments > Integrations > Vulcan integration**.



**Note:** The integration is still labeled Vulcan in Wiz. Wiz is in the process of updating this label to TenableOne.

3. On the integration page, create a new service account. The required permissions are preconfigured.
4. Click **Create**.
5. Once created, Wiz will display the access key (Client ID) and secret (Client Secret).
6. Copy both values and save them in a secure location.

You'll be required to enter the credentials in the appropriate fields in the connector set up page in Exposure Management.

- **Create or use a user with appropriate access:**

To fetch all projects, the user must have access to all Wiz projects. If you plan to fetch only specific projects, ensure the user has access to those projects.

Policies ▾ Compliance Reports Projects

## New Service Account

**Name**

What's this service account for?

**Type**  
Select which type of software component will use this Service Account

☒ Custom Integration (GraphQL API) ▾

**Projects** optional  
Limit access to selected projects only

Select Projects... ▾

Select up to 5 projects. Leave empty to grant access to all projects

**API Scopes**  
Scopes define the read and write permissions for this account.

☐ All

☐ admin:all Administrate all admin entities

☐ read:all Read all entities

☐ update:all Update all entities

☐ create:all Create all entities

☐ delete:all Delete all entities

☐ write:all Create, update and delete all entities

☐ Audit

Cancel Add

## Add a Connector

To add a new connector:

1. In the left navigation menu, click **Connectors**.
















The **Connectors** page appears.

Connectors

Search Connector Name

Select

Add new connector

Name	Connector type	Status	Last data ingestion	Created on	
 CrowdStrike111	CrowdStrike	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 NAS 946056	SmallDemoConnector	 Connected	Mar 16 2025, 05:05 PM	Jan 01 2025	Show logs
 SecurityScorecard	Security Scorecard	 Connected 	Mar 16 2025, 10:00 AM	Jan 01 2025	Show logs
 Snyk-guy	Snyk	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Acunetix Premium	Acunetix Premium	 Connecting	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 Qualys	Qualys	 Disabled	Dec 31 1969, 07:00 PM	Jan 01 2025	Show logs
 ServiceNow	ServiceNow	 Connected	Jan 05 2025, 10:02 AM	Jan 01 2025	Show logs

- In the upper-right corner, click  **Add new connector**.

The **Connector Library** appears.

Connector Library

Search Connector Name

Categories

ASM1

Asset Inventory4

Bug Bounty1

CSPM5

CWPP3

DAST8

EDR8

OT1

VM12

acunetix360

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Acunetix Premium

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

DAST

Connect

Aqua CWPP

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

CWPP

Connect

Armis

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

OT

Connect

AWS Config

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

EDR

Connect

AWS EC2

Demoing the description. This is a demo description. We will describe later. The description might be long so this is...

Asset Inventory

Connect

AWS Security Hub Standards

Axonius

Azure

- In the search box, type the name of the connector.
- On the tile for the connector, click **Connect**.

The connector configuration options appear.

## Configure the Connector



To configure the connector:

1. (Optional) In the **Connector's Name** text box, type a descriptive name for the connector.
2. (Optional) To use a preconfigured on-prem connector to connect to this connector, from the **Gateway** drop-down, select the on-prem connector you want to use for the connector. Otherwise, select **Don't use gateway**.

**Note:** For information about configuring a gateway, see [Tenable On-Prem Connector](#).

3. In the **Server Url** and **Auth Url** text boxes, paste the Wiz server and authentication URLs for your Wiz account.
4. In the **Client ID** and **Client Secret** text boxes, paste the client credentials you generated in Wiz.
5. In the **Data pulling configuration** section, you can configure dynamic settings specific to the connector.
  - In the **Fetch selected Wiz projects** text box, type the Wiz project ID from which you want to fetch data. Leave this box blank if you want to fetch data from all of your available Wiz projects.
  - In the **Asset Retention** text box, type the number of days after which you want assets to be removed from Tenable Exposure Management. If an asset has not been detected or updated within the specified number of days, it is automatically removed from the application, ensuring your asset inventory is current and relevant.

**Tip:** For more information, see [Asset Retention](#).

- (Optional) From the drop-down menu, you can choose to automatically remove assets that reach a certain asset status, for example, **Inactive** (selected by default).
6. In the **Test connectivity** section, click the **Test Connectivity** button to verify that Tenable Exposure Management can connect to your connector instance.
  - A successful connectivity test confirms that the platform can connect to the connector instance. It does not, however, guarantee that the synchronization process will succeed,





as additional syncing or processing issues may arise.

- If the connectivity test fails, an error message with details about the issue appears. Click **Show tests** for more information about the exact error.

### Test connectivity

Validate the integration connectivity prior to save and sync. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Last test (manual) was on: Mon, 31 Mar 2025 14:35:28 GMT - Success

✖ Failed tests 1 out of 4 integration tests failed

Show tests ▼

✔ Successful tests 3 out of 4 integration tests succeeded

Show tests ▼

7. In the **Connector scheduling** section, configure the time and day(s) on which you want connector syncs to occur.

**Tip:** For more information, see [Connector Scheduling](#).

8. Click **Create**. Tenable Exposure Management begins syncing the connector. The sync can take some time to complete.
9. To confirm the sync is complete, do the following:
  - Navigate to the [Connectors](#) page and monitor the [connector's status](#). Sync is complete once the connector status is **Connected**.
  - [View the sync logs](#) for the connector to monitor the logs for a successful connection.

## Wiz Vulnerabilities in Tenable Exposure Management

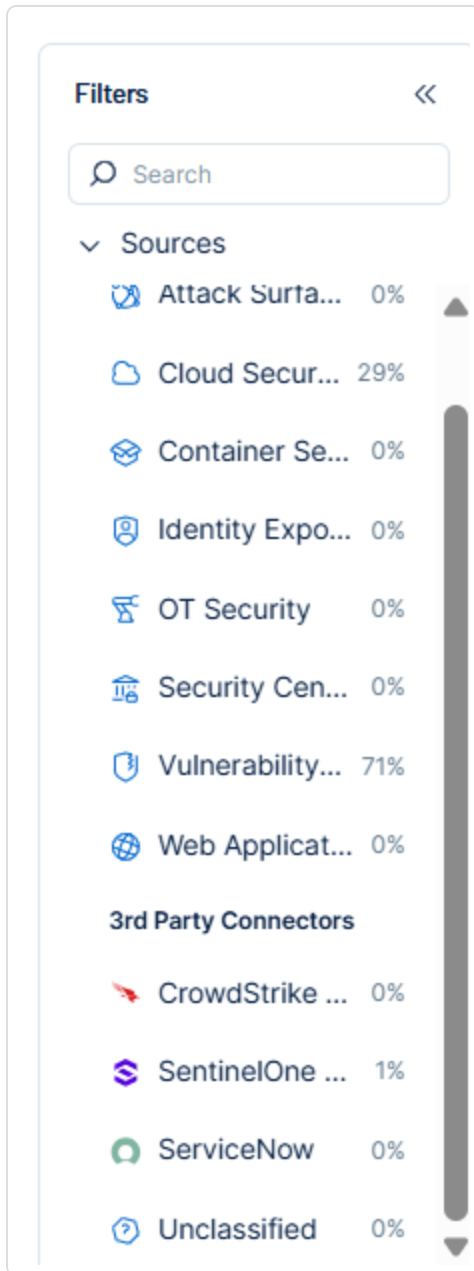
### Locate Connector Assets in Tenable Exposure Management

As the connector discovers assets, Tenable Exposure Management ingests those devices for reporting.

To view assets by connector:



1. In Tenable Exposure Management, navigate to the [Assets](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view assets.



The asset list updates to show only assets from the selected connector.

3. Click on any asset to view [Asset Details](#).

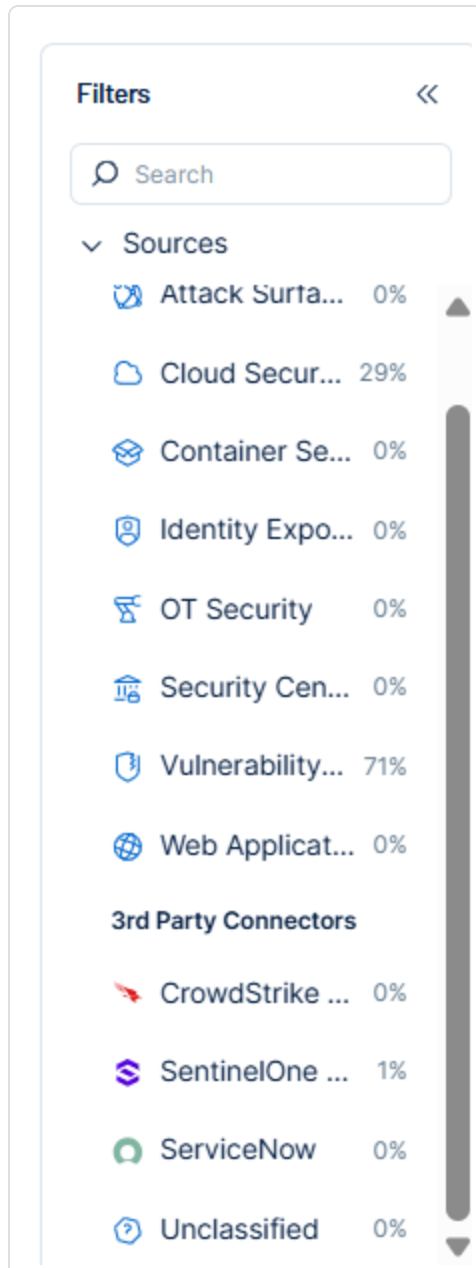
## Locate Connector Weaknesses in Tenable Exposure Management



As the connector discovers weaknesses, Tenable Exposure Management ingests those weaknesses for reporting.

To view weaknesses by connector:

1. In Tenable Exposure Management, navigate to the [Weaknesses](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view weaknesses.





---

The weaknesses list updates to show only weaknesses from the selected connector.

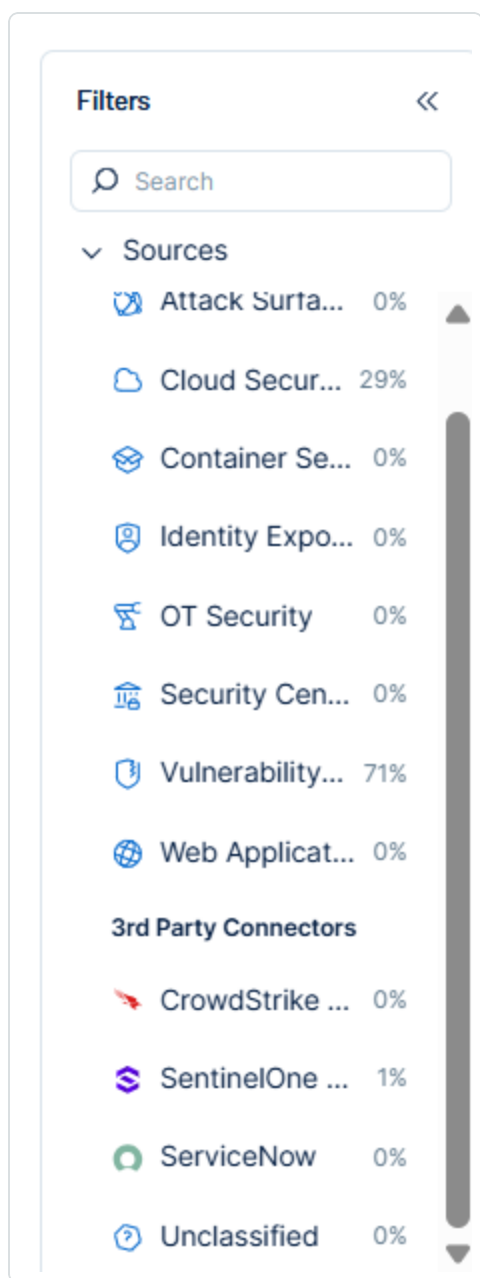
3. Click on any weakness to view [Weakness Details](#).

## Locate Connector Findings in Tenable Exposure Management

As the connector discovers individual findings, Tenable Exposure Management ingests those findings for reporting.

To view findings by connector:

1. In Tenable Exposure Management, navigate to the [Findings](#) page.
2. In the **Filters** section, under **3rd Party Connectors**, click the connector name for which you want to view findings



The findings list updates to show only assets from the selected connector.

3. Click on any asset to view [Finding Details](#).

## Data Mapping

Exposure Management integrates with the connector via API to retrieve relevant weakness and asset data, which is then mapped into the Exposure Management system. The following tables outline how fields and their values are mapped from the connector to Exposure Management.

## Device Mapping



Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Asset - External Identifier or Asset - Provider Identifier	Provider ID or External ID
Asset - Name	Name
Asset - Operating Systems	operatingSystem
Asset - IPv4 Adresses Asset - IPv6 Adresses	ipAddresses
Asset - MAC Addresses	network_interfaces.MacAddress
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral



Asset Custom Attributes	<code>os_version</code> <code>Projects</code> <code>Cloud Platform</code> <code>Region</code> <code>Subscription</code> <code>Subscription ID</code> <code>Resource Type</code> <code>Native Type</code> <code>Provider ID</code> <code>External ID</code> <code>ImageId</code> <code>PublicDnsName</code> <code>Role</code> <code>FunctionArn</code> <code>kind</code> <code>cloudProviderURL</code> <code>runtime</code> <code>status</code>
-------------------------	---

## Device Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique (Name + Provider ID + cloudProviderURL+ subscriptionExternalId)+ rule.id + Finding ID
Finding Name	rule.name



Severity Driver	severity
Finding Custom Attributes	Function As Control Finding Type:"Configurations" ID Resource External ID Resource Provider Unique ID Resource Deleted Result Status Severity Remediation
First Seen	firstSeenAt
Last seen (Observed)	analyzedAt

## Container Mapping

Wiz Container Images are mapped to Container in the Exposure Management UI.

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Asset - Name	Name
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project





	<code>cloud_platform</code> <code>Region</code> <code>Subscription</code> <code>Subscription ID</code> <code>image_source</code> <code>Wide Internet Exposure</code> <code>Image Name</code> <code>isPublic</code> <code>isEphemeral</code>
Asset Custom Attributes	<code>operatingSystem</code> <code>Images</code> <code>repoExternalId</code> <code>digest</code> <code>Projects</code> <code>Cloud Platform</code> <code>Region</code> <code>Subscription</code> <code>Subscription ID</code> <code>Resource Type</code> <code>Native Type</code> <code>Provider ID</code> <code>External ID</code> <code>ImageId</code> <code>PublicDnsName</code>



	Role
	FunctionArn
	kind
	cloudProviderURL
	runtime
	status

## Container Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique (Name + Provider ID + cloudProviderURL+ subscriptionExternalId)+ rule.id + Finding ID
Finding Name	rule.name
Severity Driver	severity
Finding Custom Attributes	Function As Control Finding Type:"Configurations" ID Resource External ID Resource Provider Unique ID Resource Deleted Result Status Severity Remediation
First Seen	firstSeenAt



Last seen (Observed)	analyzedAt
----------------------	------------

## Other Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Asset - Name	Name
Provider Names	Cloud Platform
Cloud Resource Type	Native Type
Asset - External Identifier	Provider ID
Asset - Provider Identifier	
Asset - First Observation Date	creationDate
Asset - Last Observed At	last Seen
Asset - External Tags	Tags project cloud_platform Region Subscription Subscription ID image_source Wide Internet Exposure Image Name isPublic isEphemeral



Asset Custom Attributes	Projects
	Cloud Platform
	Region
	Subscription
	Subscription ID
	Resource Type
	Native Type
	Provider ID
	External ID
	ImageId
	PublicDnsName
	Role
	FunctionArn
	kind
	cloudProviderURL

	runtime
	status

## Other Finding Mapping

Tenable Exposure Management UI Field	Wiz Field
Unique Identifier	Asset unique (Name + Provider ID + cloudProviderURL+ subscriptionExternalId)+ rule.id + Finding ID
Finding Name	rule.name
Severity Driver	severity



Finding Custom Attributes	Function As Control Finding Type:"Configurations" ID Resource External ID Resource Provider Unique ID Resource Deleted Result Status Severity Remediation
First Seen	firstSeenAt
Last seen (Observed)	analyzedAt

### Finding Status Mapping

Tenable Exposure Management Status	Wiz Status
Active	All other statuses
Fixed	Resolved Rejected

**Note:**For Wiz Configurations, Exposure Management uses the `status` field.

### Finding Severity Mapping

Tenable Exposure Management Severity	Wiz Score
Critical	Severity: Critical
High	Severity: High



Medium	Severity: Medium
Low	Severity: Low
None	Severity: Informational

**Note:** For Wiz Configurations, Tenable uses the **Severity** field to determine severity.

## Status Update Mechanisms

Every day, Tenable Exposure Management syncs with the vendor's platform to receive updates on existing findings and assets and to retrieve new ones (if any were added).

The table below describes how the status update mechanism works in the connector for findings and assets ingested into Tenable Exposure Management.

Update Type in Exposure Management	Mechanism (When?)
Archiving Assets	<ul style="list-style-type: none"><li>Asset that appears in Tenable Exposure Management and isn't returned on the next connector's sync.</li><li>Asset not seen for X days according to "Last Seen". See <a href="#">Asset Retention</a></li><li>Asset that returns from the connector with the state "Inactive" (<a href="#">configurable in Data Pulling Configuration</a>)</li></ul>
Change a Finding status from "Active" to "Fixed"	<ul style="list-style-type: none"><li>Finding status changes to <b>resolved</b> or <b>rejected</b> on the vendor's side.</li></ul>

**Note:** Updates on the vendor side are reflected in Tenable Exposure Management only when the next scheduled connector sync time is complete (once a day).

## Uniqueness Criteria

Tenable Exposure Management uses defined uniqueness criteria to determine whether an ingested asset or finding should be recognized as a distinct record. These criteria help define how assets and findings are identified and counted from each connector.



**Tip:** Read all about [Third-Party Data Deduplication in Tenable Exposure Management](#).

The uniqueness criteria for this connector are as follows:

Data	Uniqueness Criteria
Asset	Name + Provider ID + cloudProviderURL+ subscriptionExternalId
Detection	rule.id
Finding	Asset unique + Vuln unique + Finding ID

## API Endpoints in Use

API	Use in Tenable Exposure Management	Required Permissions
{{ auth_url }} /oauth/token	Generating OAuth token	None
{{ server_url }} /graphql	Create Inventory reports, Full and incrementally fetching cloud configurations findings.	create: reports read: reports read: issues

## Support Limitations and Expected Behavior

This section outlines any irregularities, expected behaviors, or limitations related to integration of the connector and Exposure Management. It also highlights details about ingested and non-ingested data to clarify data handling and functionality within this integration.

### Supported Asset Types

The Wiz connector syncs data only for the following asset types:

- Virtual Machine
- Serverless



- Container
- Container Image

### Asset Identification and Uniqueness

Asset data is retrieved from Wiz Inventory Reports using the Wiz API. These reports do not provide a consistent asset ID field. As a result, the connector uses a combination of other available fields to determine asset uniqueness.

In rare cases, this approach may lead to inaccurate aggregation or unintended deduplication of synced assets.

### Incremental Sync Logic

The connector uses the `statusChangedAt` filter to perform incremental syncs. Only the following issue changes are included:

- Newly opened issues
- Issues with a status change
- Recently resolved issues
- Ignored issues
- Issues marked as in progress

**Note:** Other updates, such as severity changes, are not included in the incremental sync.

## Data Validation

This section shows how to validate and compare data between Tenable Exposure Management and the Wiz Vulnerabilities platform.

**IMPORTANT!** Wiz data is updated frequently, which can make validation challenging. To ensure accurate comparison, include only data that aligns with the last successful sync timestamp, supported asset types, and relevant asset or finding statuses. Applying consistent filters helps maintain validation accuracy. For more info, see [Support and Limitations](#).

## Asset Data Validation





Asset data is synced using Inventory Reports via the Wiz API. For each sync, the connector generates a report titled **Tenable Inventory Report**.

**Objective:** Ensure the number of assets in **Wiz** aligns with the number of devices displayed in Tenable Exposure Management.

In Wiz:

1. Navigate to the **Reports** section.
2. Locate the most recent report named **Tenable Inventory Report**.
3. Confirm the relevant timeframe by matching the data to the timestamp of the last successful sync.
4. Filter out unsupported asset types and archived assets in Wiz. The Wiz connector only supports the following asset types: **Virtual Machine**, **Serverless**, **Container**, and **Container Image**.
5. Download the report and count the number of rows. Each row represents a single asset.

In Tenable Exposure Management:

1. [Locate your connector assets](#).
2. Compare the total number of assets between Wiz and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Wiz and Exposure Management should match.

If an asset is not visible in Exposure Management, check the following conditions:

- The asset's status changed to one of the selected statuses defined in the [Asset Retention](#) configuration (**Inactive** by default)
- Archived based on the last observed date (field **Last Seen**)

**Tip:** To learn more on how assets and findings change status, see [Wiz Issues Connector](#).

## Finding Data Validation

Configuration findings are ingested using the **CloudConfigurationFindingsPage** GraphQL query in Wiz.



**Objective:** Ensure the number of findings in Wiz aligns with the number of findings in Tenable Exposure Management.

In Wiz:

1. Navigate to the **Cloud Configuration Findings** view.
2. Filter the results to:
  - Exclude findings related to unsupported asset types.
  - Exclude archived assets.
  - Exclude findings resolved before the first fetch.
  - Match the timestamp of the last successful sync.
3. If the findings are aggregated by rule ID, sum the number of associated resources per rule to determine the total finding count.

In Tenable Exposure Management:

1. [Locate your connector findings](#).
2. Compare the total number of findings between Wiz and Tenable Exposure Management.

**Expected outcome:** The total numbers returned in Wiz and Exposure Management should match.

If a finding is missing from Exposure Management or no longer active, check the following conditions:

- The finding is marked as Fixed and appears under the Fixed state on the [Findings](#) screen.
- The finding no longer appears because its related asset was archived.

**Tip:** To learn more on how assets and findings are archived or change status, see [Wiz Issues Connector](#).

## Connector Scheduling

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).



Configuring connector sync schedules helps keep your data fresh, consistent, and aligned with your operational needs. By setting specific sync times and days, you reduce unnecessary system load, improve performance, and ensure your team has access to timely, accurate security data.

## Configure Connector Scheduling

Advanced connectors allow you to configure their synchronization time.

To configure connector sync time and days:

1. On the **Connectors** page, do one of the following:
  - [Add](#) a new connector.
  - [Edit](#) an existing connector.
2. In the **Connector Scheduling** section, set the **Sync time** and **Sync Days** to use for weekly re-occurring synchronization. At least one day must be selected.

### Connector scheduling

Set the connector syncing time and days

**Sync time**  
Initiate connector's daily sync on  UTC (00:00 AM GMT+3)

**Sync days**

MonTueWedThuFriSatSun

All week days

CancelUpdate and sync nowUpdate

3. Click **Save**.
4. After saving, you'll be prompted to choose whether to:
  - Apply the new settings for the next scheduled sync, or
  - Immediately Update and Sync Now to trigger a sync outside the schedule.

## Expected Behaviour



- **Default schedule:** New connectors default to daily sync at 11:00 PM (UTC+02:00) with all weekdays selected.
- **Editable anytime:** You can update sync time and days at any time. Changes apply starting with the next sync cycle.
- **Error recovery:** If a sync fails or is retried and runs past a non-scheduled day, it continues to completion to preserve data integrity.

## Support and Limitations

- **Supported connectors:** Most advanced connectors support scheduling. Some connectors may not display this option.
- **Single Daily Sync:** Multiple syncs per day are not supported. Each connector can sync once per scheduled day.
- **Uniform Sync Time:** The selected hour applies consistently across all selected days, and for both full and incremental (delta) syncs..

## Notes

- **Time Zone Awareness:** Sync time is configured in UTC, but is also displayed in your local browser time for clarity.
- **Hourly Precision:** You can schedule syncs on the hour only (e.g., 02:00, 16:00), making scheduling predictable and consistent.
- **Unified scheduling logic:** The same sync time applies to both full and incremental sync processes.

## Third-Party Data Deduplication in Tenable Exposure Management

Tenable Exposure Management consolidates asset and vulnerability data from both Tenable products (1st party) and third-party integrations to provide a unified, accurate asset inventory. When duplicate assets are ingested from different sources, Tenable automatically applies deduplication logic to merge records into a single asset view.



This guide explains how deduplication works for third-party data, how the system prioritizes conflicting values, and where users can view this information in the platform.

## Why Deduplication Matters

Merging duplicate assets improves clarity, reduces noise, and enables more accurate risk assessment. In Tenable Exposure Management, deduplication happens automatically across sources, giving you:

- A single source of truth for each asset.
- Complete visibility into merged properties from all integrated platforms.

## How it Works

Tenable Exposure Management achieves asset deduplication by crossing complex merge criteria and identifying duplications across the data ingested from the different sources.

The merging mechanism is designed to avoid disassembling and reassembling Tenable Exposure Management assets. If the merging criteria are met, new data is added to the existing structure.

**Note:** At this stage, Tenable Exposure Management uses a predefined merge strategy and property matching logic. Customization of merge rules is not currently available, but enhancements are planned for future releases.

Assets that are deduplicated and merged are considered **Multi Source Assets**. For more information, see [View License Information](#) in the *Tenable Vulnerability Management User Guide*.

## Deduplication Criteria by Asset Class

Tenable applies a default merge strategy per asset class, using key properties to match and merge assets. The deduplication logic is case-insensitive and includes parsing of common formats (e.g., MAC addresses, hostnames).

**Tip:** For more information, see [Asset Classes](#).

Asset Class	Default Merge Properties (in order of priority)
Device	1. External Identifier



	<ol style="list-style-type: none"><li>2. Mac Addresses</li><li>3. Name + FQDNs + IP Addresses</li><li>4. Name + FQDNs</li><li>5. FQDNs + IP Addresses</li><li>6. Name + IP Addresses</li><li>7. Name</li></ol>
Container	<ol style="list-style-type: none"><li>1. sha256</li><li>2. name</li></ol>
Web Application	<ol style="list-style-type: none"><li>1. Webapp Homepage Screenshot Url</li><li>2. Name</li></ol>
Cloud Account Role Group Storage Resource Other	External Identifier

**Important!** The merge criteria listed in this document apply only to third-party data (data ingested from [Connectors](#)).

Tenable-native assets, such as the data that comes from Tenable Vulnerability Management, follow separate internal deduping logic.

**Important!** Assets with different Tenable UUIDs will never be merged, even if all other third-party matching criteria are met. This safeguards the integrity of Tenable-managed assets and prevents unintended merges.

## Property Merge Order



When multiple sources provide different values for the same property (for example, conflicting IP addresses or operating systems), Tenable uses a fixed priority order to determine which value appears in the unified view.

## Default Merge Priority

1. Tenable-native sources (such as Tenable Vulnerability Management) take precedence.
2. Third-party [Connectors](#) are prioritized by the order they were connected. The first connected source is used unless its value is missing, in which case the next available source is used.

**Note:** The order of connectors influences the merging process. The first connector that completes processing within Tenable Exposure Management determines the identifying criteria.

## Example

An asset is discovered by:

- Tenable Vulnerability Management
- CrowdStrike (connected second)
- Microsoft Defender for Endpoint (connected third)

Each source reports different values for IP address and operating system:

Property	Tenable Vulnerability Management	CrowdStrike	Microsoft TVM
IP Address	10.0.0.1	172.16.5.10	192.168.1.100
Operating System	Windows 10 Pro	Windows 11	Windows 10 Enterprise

Result:

- The IP address and OS from Tenable Vulnerability Management are selected and displayed in the UI.
- The values from CrowdStrike and Microsoft TVM are still stored and viewable in the [Asset Details](#) tab but are not shown by default.



## Deduplication Limitations

- Assets must belong to the same class to be merged. For example, two assets from different connectors won't merge if one is an Account and the other is a Role.
- For cloud assets, provider IDs may differ by vendor. For example:
  - AWS via one connector might use full ARN
  - Another might use a shortened ID
  - Tenable supports matching multiple keys via a list-based `NATIVE_ID`.

## Additional Resources

- [Asset Deduplication FAQ](#)

## Asset Retention

Effective risk remediation involves focusing on what matters most to your organization. To keep your lists of assets and weaknesses as fresh and relevant as possible and minimize false positives, Tenable Exposure Management automatically removes assets that are presumed to be retired or inactive and represent no risk to your organization.

## Configuring Asset Retention

Tenable Exposure Management provides asset retention settings that let you control when an asset is considered inactive and eligible for removal. This can be configured individually for each connector on its setup page.

To configure asset retention of a specific connector:

1. Within Tenable Exposure Management, navigate to **Connectors**.
2. In the connectors list, click on the connector for which you want to configure asset retention.  
  
The edit connector page appears.
3. In the **Asset Retention** section, configure the retention period for inactive assets based on their last seen date. If an asset has not been detected or updated in a scan within the





specified days, Tenable Exposure Management automatically removes it. This ensures your asset inventory stays current and relevant.

### Asset Retention

Remove assets when their last seen date is more than  days ago

Immediately remove assets when their status is:

Inactive



NoSensorData



**Tip:** Some connectors allow you also to configure the asset retention based on status change.

## How long after the last sync is an asset considered inactive?

Asset inactivity represents the configuration of the number of days Tenable Exposure Management waits before removing an asset once its no longer present in a scan. If your scan cycles are less frequent and you want to keep assets around for longer periods of time, choose a higher number of days, for example, 90.

If you scan multiple times a day with total coverage and want assets removed as soon as they are missing from a scan, choose a lower value, like 1.

Tenable defines the time an asset was last seen by the *Last Seen* time ingested from the native tool, if available. Otherwise, Tenable pulls from the most recent time the connector synced with Tenable Exposure Management.

## Tenable Exposure Management Cloud Sensors

[Tenable Exposure Management connectors](#) use the following IPs ranges per container region in order to facilitate sync communication. If using tool side allowlisting, make sure to have these addresses for your region added in advance of your first sync.

The following table identifies each regional cloud sensor and, for allow list purposes, its IP address ranges. These IP address ranges are exclusive to Tenable.



**Tip:** The cloud sensor and IP address information contained in the table below is also [provided in JSON format](#) for users that want to parse the data programmatically.

Sensor Region	IPv4 Range	IPv6 Range
ap-northeast-1	13.115.104.128/25 35.73.219.128/25	2406:da14:e76:5b00::/56
ap-southeast-1	13.213.79.0/24 18.139.204.0/25 54.255.254.0/26	2406:da18:844:7100::/56
ap-southeast-2	13.210.1.64/26 3.106.118.128/25 3.26.100.0/24	2406:da1c:20f:2f00::/56
ap-south-1	3.108.37.0/24	2406:da1a:5b2:8500::/56
ca-central-1	3.98.92.0/25 35.182.14.64/26	2600:1f11:622:3000::/56
eu-west-1	3.251.224.0/24	2a05:d018:f53:4100::/56
eu-west-2	18.168.180.128/25 18.168.224.128/25 3.9.159.128/25 35.177.219.0/26	2a05:d01c:da5:e800::/56
eu-central-1	18.194.95.64/26 3.124.123.128/25 3.67.7.128/25 54.93.254.128/26	2a05:d014:532:b00::/56
me-central-1	51.112.93.0/24	2406:da17:524:dd00::/56
us-east-1	34.201.223.128/25 44.192.244.0/24 54.175.125.192/26	2600:1f18:614c:8000::/56
us-east-2	13.59.252.0/25	2600:1f16:8ca:e900::/56



Sensor Region	IPv4 Range	IPv6 Range
	18.116.198.0/24 3.132.217.0/25	
us-west-1	13.56.21.128/25 3.101.175.0/25 54.219.188.128/26	2600:1f1c:13e:9e00::/56
us-west-2	34.223.64.0/25 35.82.51.128/25 35.86.126.0/24 44.242.181.128/25 35.93.174.0/24	2600:1f14:141:7b00::/56
sa-east-1	15.228.125.0/24	2600:1f1e:9a:ba00::/56
static	162.159.129.83/32 162.159.130.83/32	2606:4700:7::a29f:8153 2606:4700:7::a29f:8253

Regional cloud sensors appear in the following groups:

- **US East Cloud Scanners:** A group of scanners from the us-east-1 (Virginia) or the us-east-2 (Ohio) ranges.
- **US West Cloud Scanners:** A group of scanners from the us-west-1 (California) or the us-west-2 (Oregon) ranges.
- **AP Singapore Cloud Scanners:** A group of scanners from the ap-southeast-1 (Singapore) range.
- **AP Sydney Cloud Scanners:** A group of scanners from the ap-southeast-2 (Sydney) range.
- **AP Tokyo Cloud Scanners:** A group of scanners from the ap-northeast-1 (Tokyo) range.
- **CA Central Cloud Scanners:** A group of scanners from the ca-central-1 (Canada) range.
- **EU Frankfurt Cloud Scanners:** A group of scanners from the eu-central-1 (Frankfurt) range.
- **UK Cloud Scanners:** A group of scanners from the eu-west-2 (London) range.
- **Brazil Cloud Scanners:** A group of scanners from the sa-east-1 (São Paulo) range.



- **India Cloud Scanners:** A group of scanners from the ap-south-1 (Mumbai) range.
- **Amazon GOV-CLOUD:** A group of scanners available for Federal Risk and Authorization Management Program (FedRAMP) environments.
- **US Cloud Scanner:** A group of scanners from the following AWS ranges:
  - us-east-1 (Virginia)
  - us-east-2 (Ohio)
  - us-west-1 (California)
  - us-west-2 (Oregon)
- **APAC Cloud Scanners:** A group of scanners from the following AWS ranges:
  - ap-northeast-1 (Tokyo)
  - ap-southeast-1 (Singapore)
  - ap-southeast-2 (Sydney)
  - ap-south-1 (Mumbai)
- **EMEA Cloud Scanners:** A group of scanners from the following AWS ranges:
  - eu-west-1 (Ireland)
  - eu-west-2 (London)
  - eu-central-1 (Frankfurt)
  - me-central-1 (UAE)
- **UAE Cloud Scanners:** A group of scanners from the me-central-1 range.

## Connectors FAQ

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The following are frequently asked questions regarding connectors in Tenable Exposure Management.



## Integration and Support

### What integrations does Tenable Exposure Management support?

Tenable Exposure Management supports a wide range of integrations, as detailed in [Supported Third-Party Integrations](#).

### What if my security tool doesn't have a dedicated connector?

If there isn't a dedicated connector for your security tool, you can use the [Tenable On-Prem Connector](#) to upload vulnerability data via CSV files.

### Does Tenable Exposure Management support mobilization (ticketing systems) connectors?

Currently, Tenable Exposure Management does not support integrations with ticketing tools.

## Sync and Status

### How can I identify the status of my connector?

Once a connector is configured, you can monitor its status in the following ways:

- See [Connector Data Status](#)
- See [Connector Logs](#)

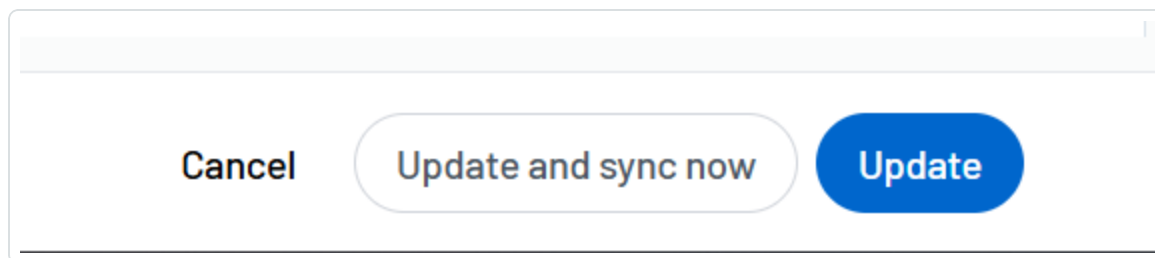
### How can I re-sync a connector on demand?

You can manually trigger a sync for connectors. Sync buttons are available on the connector's setup page:

- **Sync Now:** Triggers a sync without saving changes.
- **Update:** Saves connector settings but waits for the next scheduled sync.



- **Update and Sync Now:** Saves the changes and starts syncing immediately.



## Can I sync or process more than one connector at a time?

Yes. Tenable Exposure Management allows you to run syncs for multiple connectors at the same time.

The platform supports parallel sync execution, meaning you can trigger multiple connector syncs—manually or through scheduled jobs—without waiting for one to finish before starting another. View the [Connector Logs](#) to track each sync's progress.

## What can I expect during a sync?

Sync duration varies by vendor and data volume. The [Connector Logs](#) tab is the most reliable way to confirm sync completion or investigate errors.

## Deleted Connectors and Tags

**Important!** Full syncs can take up to 24 hours, at which point all connector data is fully removed from Tenable Exposure Management and its user interface.

## What happens to asset and vulnerability data when I delete a connector?

When you delete a connector, Tenable Exposure Management removes all native data ingested through that specific integration.

This includes assets, weaknesses/findings, and data metadata fields associated with the connector:

- Only the data unique to that connector is removed.
- If another active connector provides the same asset or finding, that data remains visible and valid in the platform.



## When is the data actually deleted?

Tenable Exposure Management removes the data in two stages:

- **Immediately after deletion:** The connector is removed from the UI, and its data is marked for deletion.
- **Next day:** The data is purged during the next scheduled backend cleanup, in line with the Tenable data retention process.

## What happens to historical dashboards and reports?

Data previously included in [dashboards](#) or reports may still appear until Tenable Exposure Management refreshes the dataset or clears cached data.

Keep in mind:

- These records are not live.
- You won't see the deleted connector listed in current queries or filters.

## Does the deleted data still show up in the Inventory view?

No. Once the connector is deleted and the data is purged, the associated assets and vulnerabilities will no longer appear in:

- [Inventory](#)
- [Exposure View](#)
- [Exposure Signals](#)
- [Dashboards](#) (after data refresh)

## Can I recover a deleted connector or its data?

No. Once a connector is deleted and the data retention period has passed, the data is permanently removed. To restore access to the data, you must:

1. Reconfigure the connector.
2. Allow the sync to complete to reingest the data into Tenable Exposure Management.



**Note:** Some data (such as historical risk scores or past exceptions) may not fully reappear depending on the connector's design and sync behavior.

## How do I confirm that a connector has been deleted?

After deletion:

- The connector disappears from the **Connectors** page.
- Its source tag or icon is removed from the **Inventory** and **Asset Details** views.
- The connector no longer appears as a **Source** for any active assets.

## Is the data deletion process the same for all connectors?

Yes. The same deletion logic applies to both first-party and third-party connectors. Only data that was originally ingested by the deleted connector is be removed from Tenable Exposure Management.

## How long does Tenable Exposure Management keep my connector data in my Dashboards?

By default, Tenable Exposure Management retains dashboard data within the user interface for 90 days. To access this data after this point, contact your Tenable representative.

## Asset Deduplication FAQ

The following are frequently asked questions regarding asset deduplication in Tenable Exposure Management.

**Important:** The following content refers to automatic deduplication for assets from different sources. For information about enabling the automatic deduplication of assets from the same source, see **Settings** > [Same Source Asset Deduplication](#).

## Do Tenable-native assets follow the same merge criteria as third-party data?

No. Tenable-native assets use a separate, internal merging logic that is not configurable or visible in the platform. The merge criteria [documented in this guide](#) apply only to assets ingested from third-party connectors.





Additionally, assets with different Tenable UUIDs are never merged, even if all other matching fields (such as hostname or IP address) align. This ensures accurate separation of Tenable-managed data and prevents unintended merging between unrelated records.

## What happens when I add additional connectors with asset data?

If the deduplication criteria are met, the data merges from multiple connectors into a single asset. These are considered **Multi Source Assets**. For more information, see [View License Information](#) in the *Tenable Vulnerability Management User Guide*.

If the criteria aren't met, the platform treats the asset as unique and creates a new record in the inventory.

## How does the system decide whether to merge asset data?

Tenable Exposure Management uses fixed matching criteria per asset class (e.g., device, website). If at least one combination of matching fields meets the merge conditions, the platform merges the data into a single asset.

**Example for devices:** If two connectors report the same hostname + IP + FQDN, the assets may be merged.

## Can I customize the merge criteria?

No. The merge logic and field combinations are currently predefined and not configurable. Custom merge strategies may be introduced in future releases.

## Can I choose which connector takes priority for conflicting data?

No. Tenable uses a fixed information order:

1. Tenable-native sources take priority.
2. Third-party connectors are prioritized by the order they were added to the system.

You can review the source of each field on the **Connector Details** tab of the [Asset Details](#) page.

## What happens if multiple connectors sync at the same time?



The platform doesn't queue syncs but processes them concurrently. The first successfully processed connector becomes the primary source for merge decisions if Tenable-native data is not available.

## Why do I still see data from a removed connector?

If an asset was merged and the connector is deleted, Tenable Exposure Management retains the merged data if other sources still report matching values. Only data exclusively ingested by the deleted connector is removed during connector deletion.



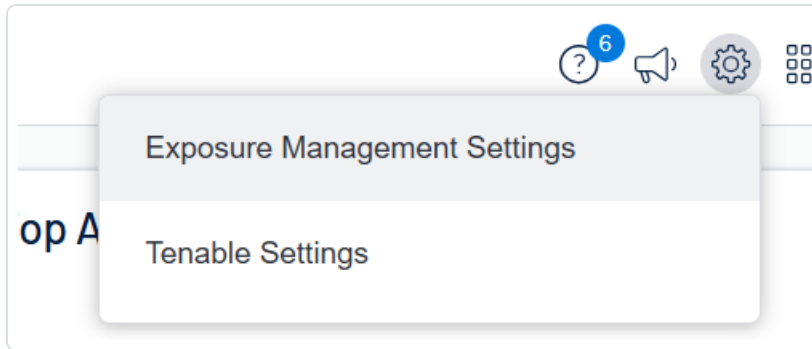
## Settings

Within Tenable Exposure Management, you can manage your Tenable Exposure Management settings as well as navigate directly to the Tenable Vulnerability Management interface to manage your Tenable One platform settings.

To access Settings:

1. In the upper-right corner of any page, click the  button.

A menu appears.



2. Do one of the following:

- To manage your Tenable Exposure Management settings, click **Exposure Management Settings**.

The **Exposure Management Settings** page appears. For more information, see [Exposure Management Settings](#).

- To manage your Tenable One platform settings, click **Tenable Settings**.

You navigate directly to the **Settings** page within Tenable Vulnerability Management. For more information, see [Settings](#) in the *Tenable Vulnerability Management User Guide*.

## Exposure Management Settings

The Exposure Management Settings page allows you to configure Tenable Exposure Management specific options:

To access the Exposure Management Settings page:



1. In the upper-right corner of any page, click the  button.

A menu appears.

2. Click **Exposure Management Settings**.

The **Exposure Management Settings** page appears.

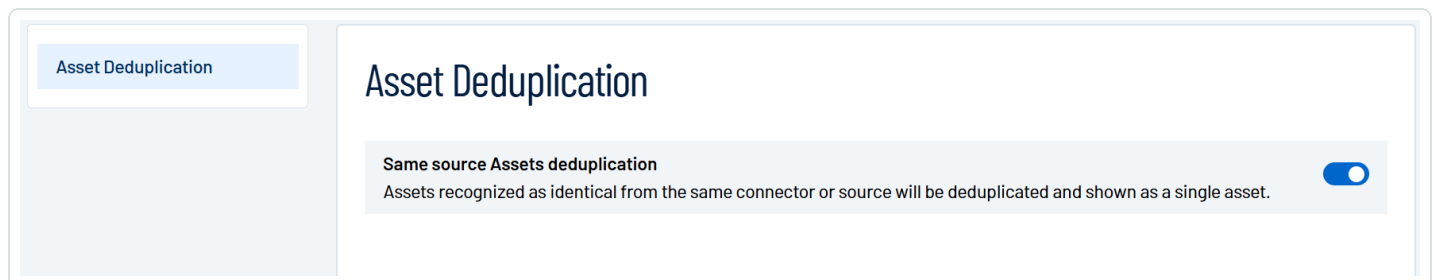
Here, you can configure the following Exposure Management specific options:

## Same Source Asset Deduplication

**Important:** The following content refers to automatic deduplication for assets from **the same** source. For information about the automatic deduplication of assets from **different** sources, see [Third-Party Data Deduplication in Tenable Exposure Management](#).

Merging duplicate assets improves clarity, reduces noise, and enables more accurate risk assessment. The **Asset Deduplication** setting allows you to merge identical assets from separate sources into one asset cluster. This can be helpful when you want to:

- Merge multiple assets from one connector source.
- Merge multiple assets from 2 or more instances of the same connector.



You can view this logic and related data in the [Asset Cluster Logic](#) section of the **Asset Details** page.

To configure Asset Deduplication:

1. On the **Exposure ManagementSettings** page, click the **Asset Deduplication** tab.

The **Asset Deduplication** configuration options appear.

2. Choose one of the following options:



- **Disabled** (Default) – Each asset, regardless of its source, remains separated throughout Tenable Exposure Management.
- **Enabled** – Each asset from the same source (connector instance) is merged into a single asset cluster.

3. Click **Save**.

Tenable Exposure Management applies your changes.