

A network diagram background consisting of a complex web of interconnected nodes and lines, rendered in shades of blue and white. The nodes are represented by small circles, and the lines are thin, connecting the nodes in a non-linear fashion. The overall effect is a sense of connectivity and data flow.

CipherInsights™

From QUANTUMXCHANGE

SYSTEM REFERENCE GUIDE

Software Version 10.1

Table of Contents

1 Introduction1

2 Cyber Risk2

2.1 Run a Risk Assessment 2

2.2 Dashboard View 3

2.3 Evaluating Risk Data 4

2.3.1 Identity Risk 4

2.3.2 Device Risk 5

2.3.3 Network Risk 5

2.3.4 Application Risk 8

2.3.5 Data Risk 9

2.4 Risk Adjustments 10

3 Zero Trust12

3.1 Encryption Visibility 12

3.1.1 Dashboard Details 13

3.2 Digital Certificates 14

3.2.1 Dashboard Details 14

4 Discover18

4.1 Violations 24

4.2 Sessions 24

4.3 Nodes 25

4.4 Certificate Chains 25

4.5 Certificates 26

4.6 Certificate Authorities 27

4.7 Invalid Certificates 27

5 Explore28

6 Report30

6.1 Asset Counting 31

6.2 Book Reports 32

6.3 Certificate Expirations 33

6.4 Certificate Wildcards 34

6.5 Clear vs Encrypted Traffic 35

6.6 Dta Report 36

6.7 Endpoint Network Traffic 37

6.8 Recent Database or Client Activity 39

6.9 SSL/TLS Usage 40

6.10 Self-Signed and Untrusted Certificates 41

6.11 TLS Cipher Suite Usage 42

7 Certificate Validation43

7.1 Certificate Sources 43

7.2 Validation Settings 44

7.3 Updating Individual Certificate Settings 45

8 System Alerts46

Certificate of Compliance48

1 Introduction

This document describes the features and functionality of the CipherInsights product. The expectation is that the system has already been installed and configured using the CipherInsights ISO Installation Guide and the CipherInsights Analytics Hub Configuration and Management Guide.

The CipherInsights application provides a comprehensive automated internal assessment across 7 risk factors from endpoints and authentication at the edge to the application servers and databases in the network core, along with all the protocols connecting them.

Each risk factor is scored from 0 to 100, with 100 being the highest risk. The score is derived by assessing the vulnerabilities associated with each risk factor. Each vulnerability is cataloged, and objective evidence is collected to drive remediation efforts both internally and on network-connect third parties.

The CipherInsights application also provides a Zero Trust visibility solution for encryption and digital certificate visibility of encrypted traffic in motion, when the associated license is installed.

Zero Trust features include:

- Automatic identification of encrypted and unencrypted traffic, at a macro level, down to session.
- Advanced filtering for the investigation of both encrypted and unencrypted traffic of on-net or off-net traffic in both cloud and on-prem deployments.
- Discovery of all certificates that are in use inside a company's infrastructure.
- Identification of certificates that are self-signed, contain wildcards or are expired and still being actively used.
- Reporting of the session usage count of various TLS versions, so older versions can be acted upon and removed, enabling enforcement of security policy through active visibility.
- Display of all certificate authorities actively being used inside the infrastructure (valid, invalid, unknown).
- A discovery workbench to drill and trace into the session information including:
 - List un-encrypted servers on net
 - List obsolete TLS 1.0, 1.1 versions in use
 - List self-signed certs in use
 - List wildcard certs in use
 - List expired certs in use
- Real-time processing of TCP sessions enables continuous discovery of all active servers responding to connection attempts and their associated clients.
- Tabular and visual summaries and drill downs through a web console and an extensive set of analytical reports to enable alignment of your encryption environment with best practices for securing data.
- Identification of all databases in use in the network.
- Ability to map applications based on certificate use.

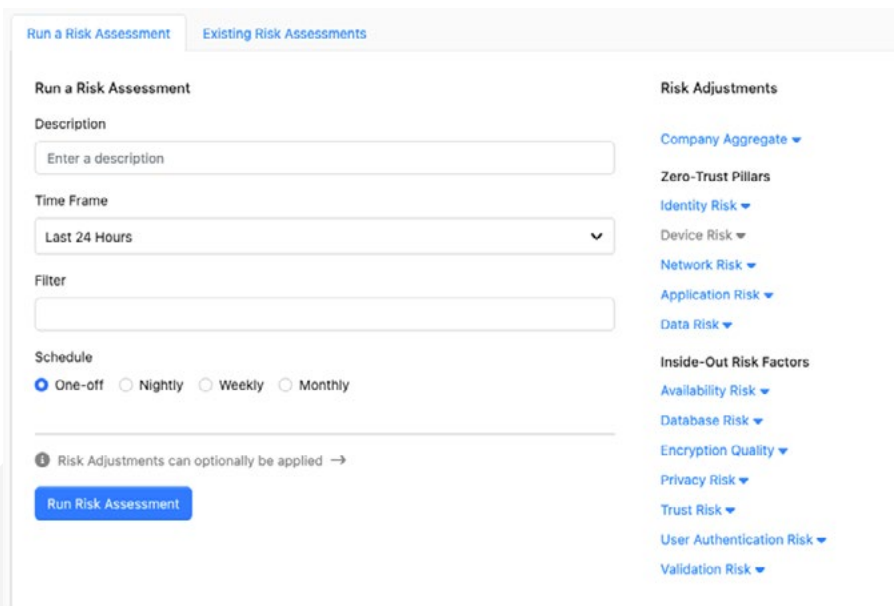
This guide assumes the reader is familiar with logging in and navigating through the system. For detailed instructions on system navigation, see the *CipherInsights Analytics Hub Configuration and Management Guide*.

2 Cyber Risk

When the user logs in to the CipherInsights application for the first time, they will be taken to the Cyber Risk page. After allowing the system to collect data for a short period of time, one week is recommended, the first step of the evaluation process is to run an assessment to generate the scorecard and dashboard view.

2.1 Run a Risk Assessment

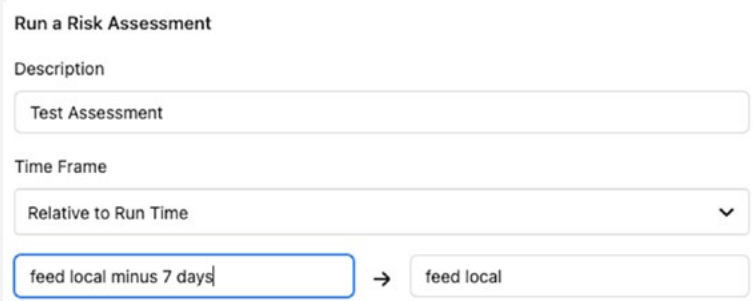
As stated above, the first step in the Cyber Risk evaluation process is to run a risk assessment. The initial landing page will display the risk assessment configuration page on first log in.



Fill out each of the fields to run the assessment:

Description and Timeframe

To run a one-week assessment, select a timeframe using Relative to Run Time and then set the start time to feed local minus seven days.



Description and Timeframe

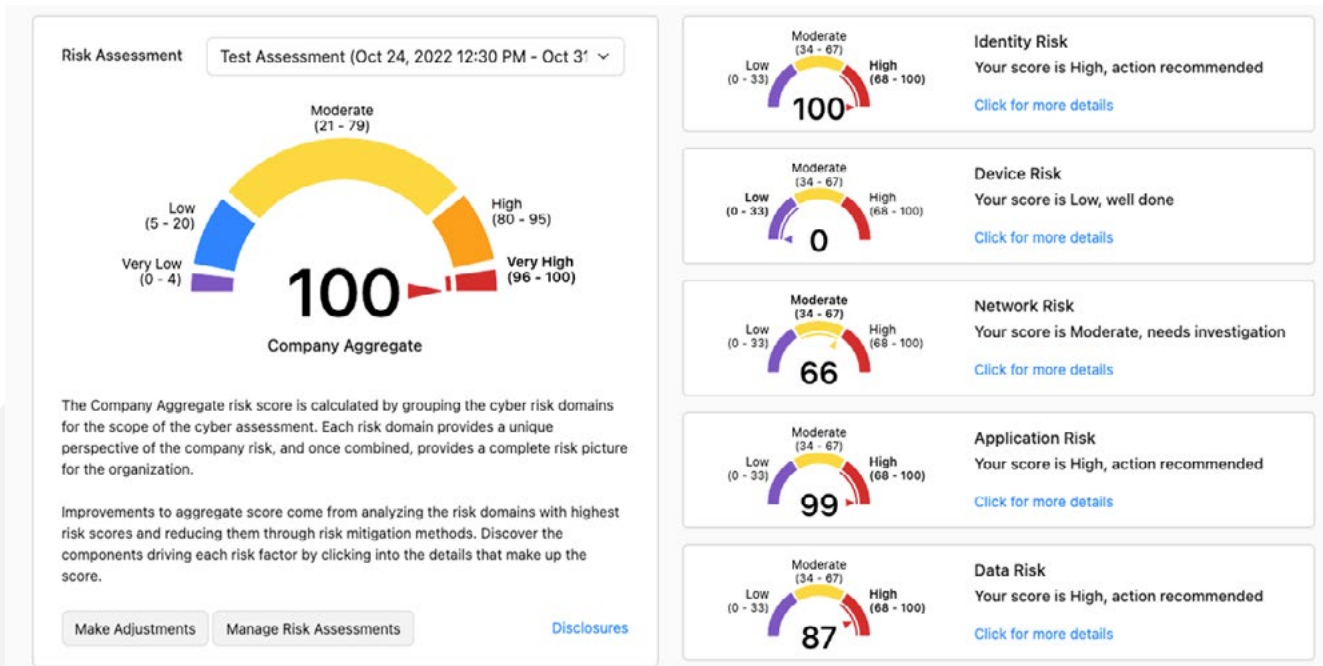
Run the initial assessment as One-off. Once you have evaluated the overall score you can adjust and then schedule on a nightly, weekly, or monthly basis.

Schedule

One-off
 Nightly
 Weekly
 Monthly

2.2 Dashboard View

Once an assessment has been run, the system will display the assessment report dashboard.



The left side of the screen provides the company aggregate score. The default configuration sets this score as the maximum of the five pillar scores calculated by the system. The reason for this being your overall security, and associated risk, is only as strong as the weakest link.

The right side of the dashboard provides the scores for the five pillars of the CISA Zero Trust maturity model.

- Identity Risk
- Device Risk
- Network Risk
- Application Risk
- Data Risk

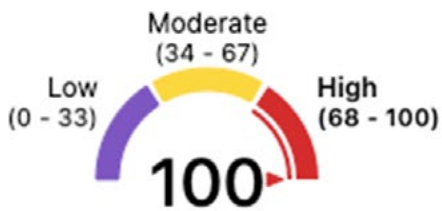
Each pillar has one or more risk factors that are evaluated and averaged to provide a risk score for that pillar.

2.3 Evaluating Risk Data

Each risk pillar has multiple factors used to calculate the overall score. At the pillar level, the scores are averaged to generate the pillar risk score.

2.3.1 Identity Risk

The Identity Risk score evaluates authentication and authorization risk in the network.

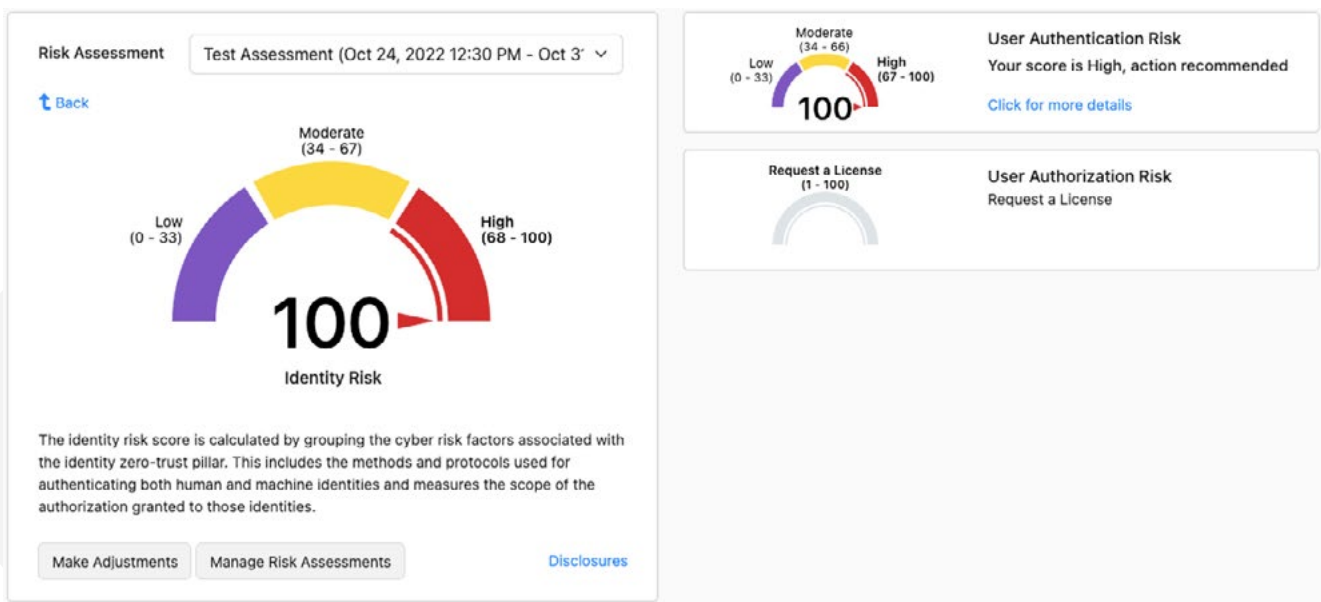


Identity Risk

Your score is High, action recommended

[Click for more details](#)

The score is made up of the average of the User Authentication Risk Score and the User Authorization Risk Score.



Risk Assessment Test Assessment (Oct 24, 2022 12:30 PM - Oct 31, 2022) ▾

[Back](#)

Moderate (34 - 67)
Low (0 - 33) High (68 - 100)
100
Identity Risk

The identity risk score is calculated by grouping the cyber risk factors associated with the identity zero-trust pillar. This includes the methods and protocols used for authenticating both human and machine identities and measures the scope of the authorization granted to those identities.

[Make Adjustments](#) [Manage Risk Assessments](#) [Disclosures](#)

Moderate (34 - 66) High (67 - 100)
Low (0 - 33)
100

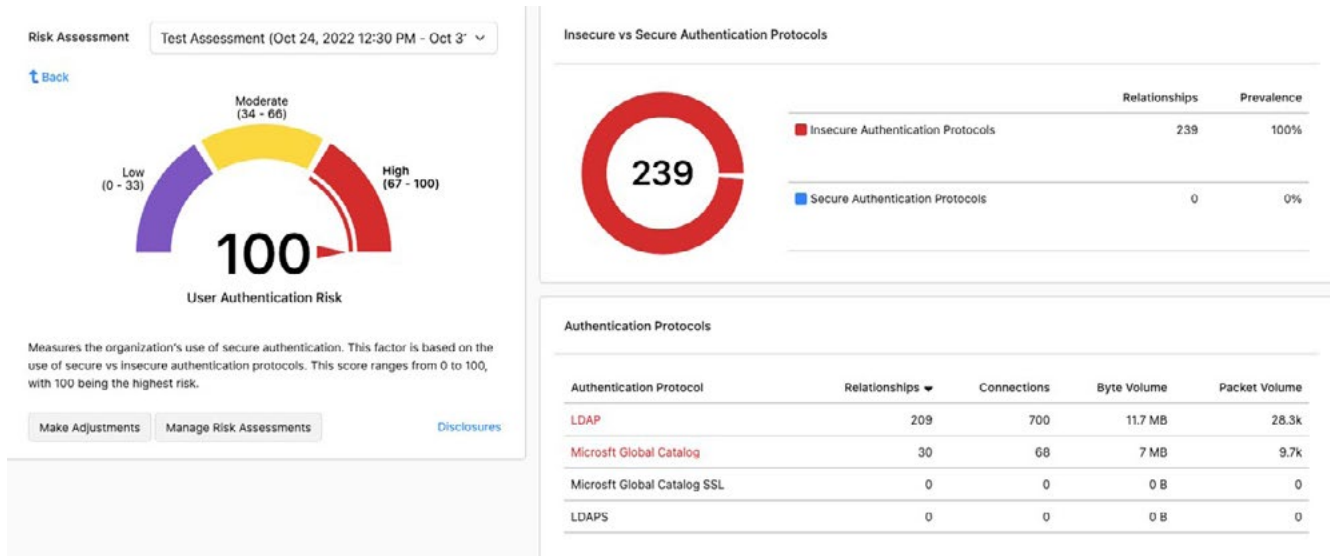
User Authentication Risk
Your score is High, action recommended
[Click for more details](#)

Request a License (1 - 100)

User Authorization Risk
Request a License

User Authentication Risk

The Authentication Risk score is based on insecure vs secure forms of user authentication in the network under evaluation. The application looks for relationships using LDAP vs LDAPs and Microsoft Global Catalog vs Microsoft Global Catalog SSL.



User Authorization Risk

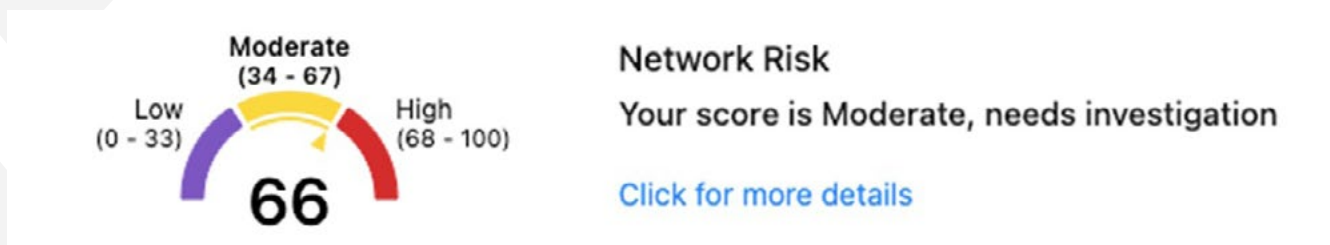
The User Authorization Risk score is based on least-privilege, i.e., the number of endpoints accessing internal servers. This scorer is still under development and is not used in scoring in this version of the software.

2.3.2 Device Risk

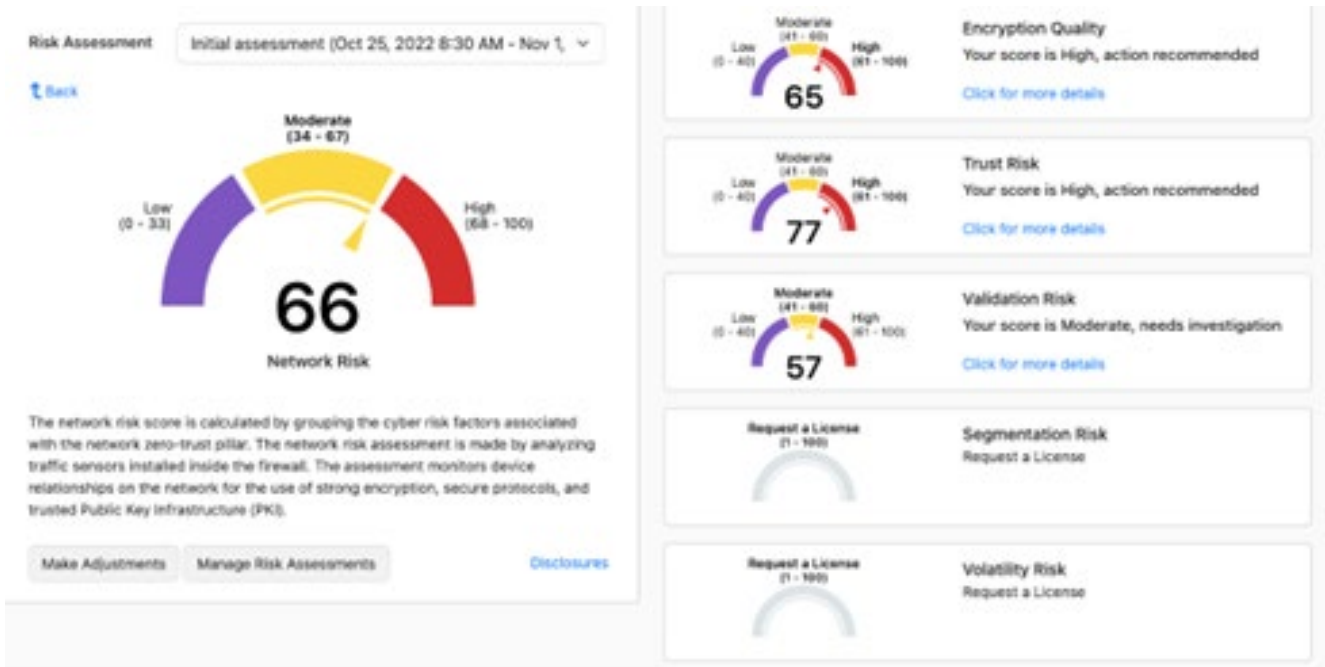
The Device Risk pillar is still under development and is not used in scoring in this version of the software.

2.3.3 Network Risk

The Network Risk score evaluates encryption, certificate trust, and certificate validation in the network.

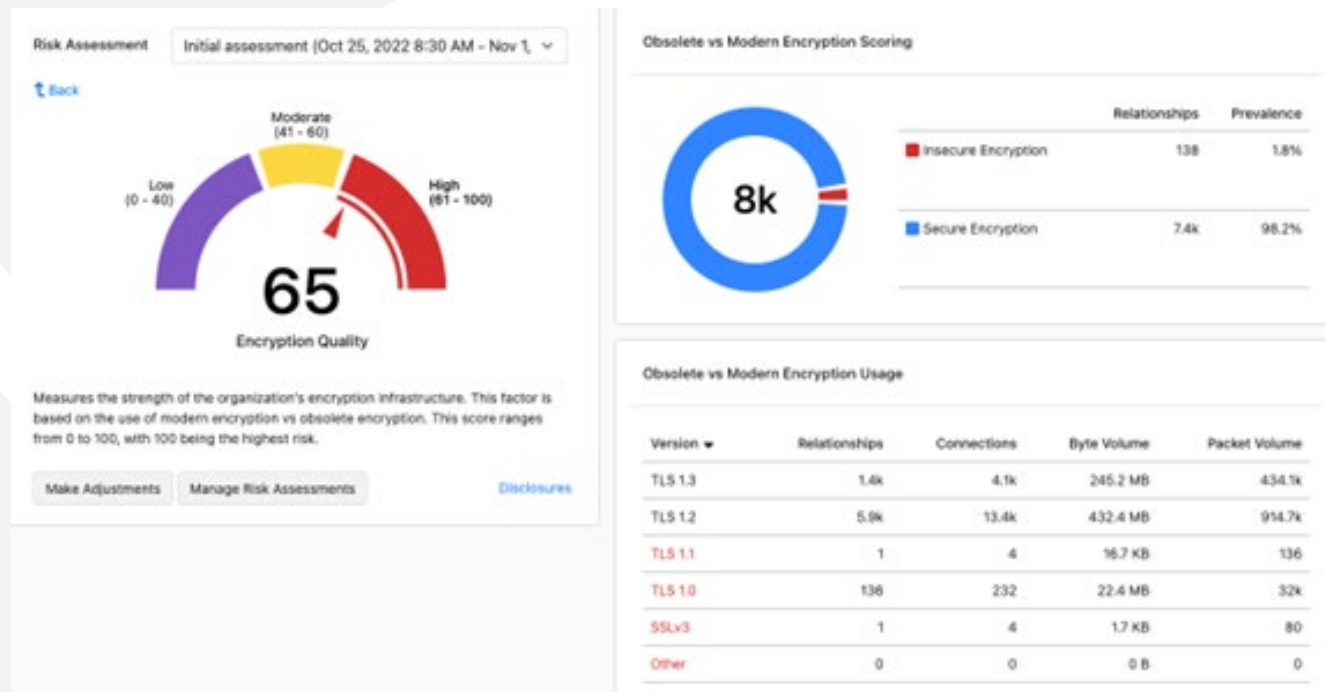


The score is made up of the average of the Encryption Quality, Certificate Trust, Certificate Validation, Segmentation, and Volatility Risk scores.



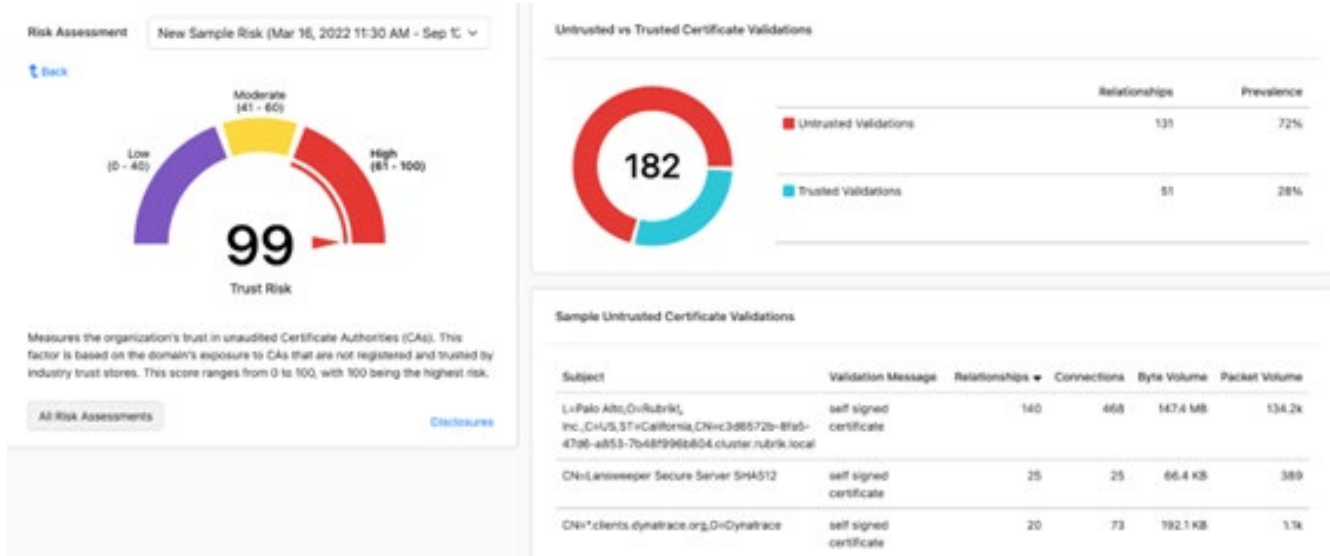
Encryption Quality

The Encryption Quality scorer evaluates SSL and TLS usage in the network. Use of modern encryption – TLS1.2 and TLS1.3 are scored positively. Use of obsolete encryption including SSLv3, TLS1.0, and TLS1.1 put the network at risk and are identified for potential remediation.



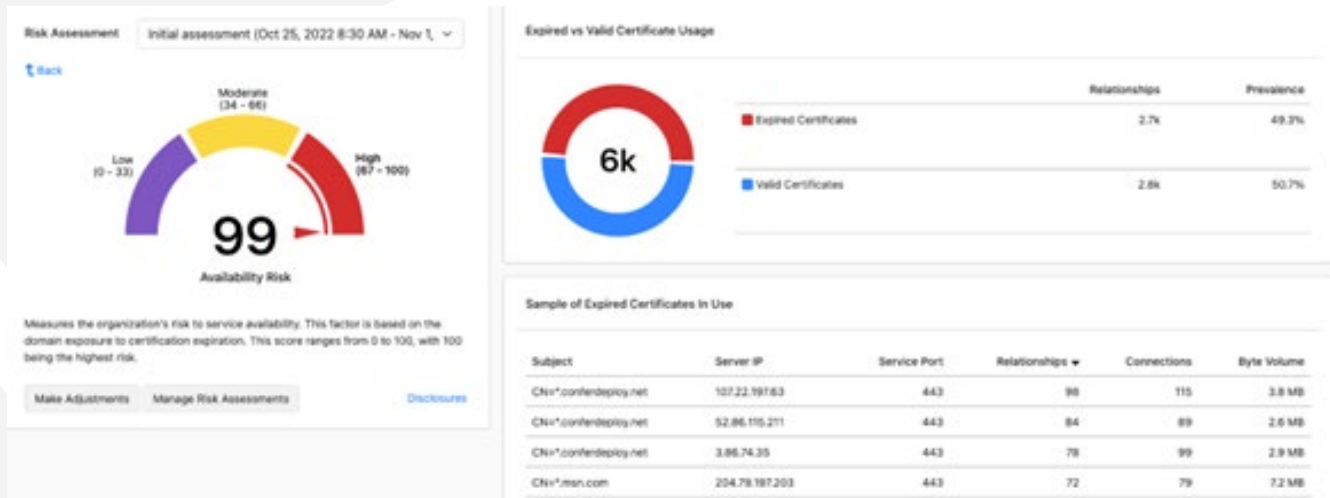
Trust Risk

The Trust Risk scorer evaluates certificates to identify self-signed vs trusted third party certificate usage in the network. Hackers use self-signed certificates to encrypt data for exfiltration from customer networks.



Validation Risk

The Validation Risk scorer evaluates certificates and certificate chains. The CipherInsights system attempts to validate certificate chains to the root certificate of trust. If the root certificate cannot be found or identified, then the certificate chain is invalid.



Segmentation Risk

The Segmentation Risk scorer is still under development at this time and is not used in risk scoring at this time.

Volatility Risk

The Volatility Risk scorer is still under development at this time and is not used in risk scoring at this time.

2.3.4 Application Risk

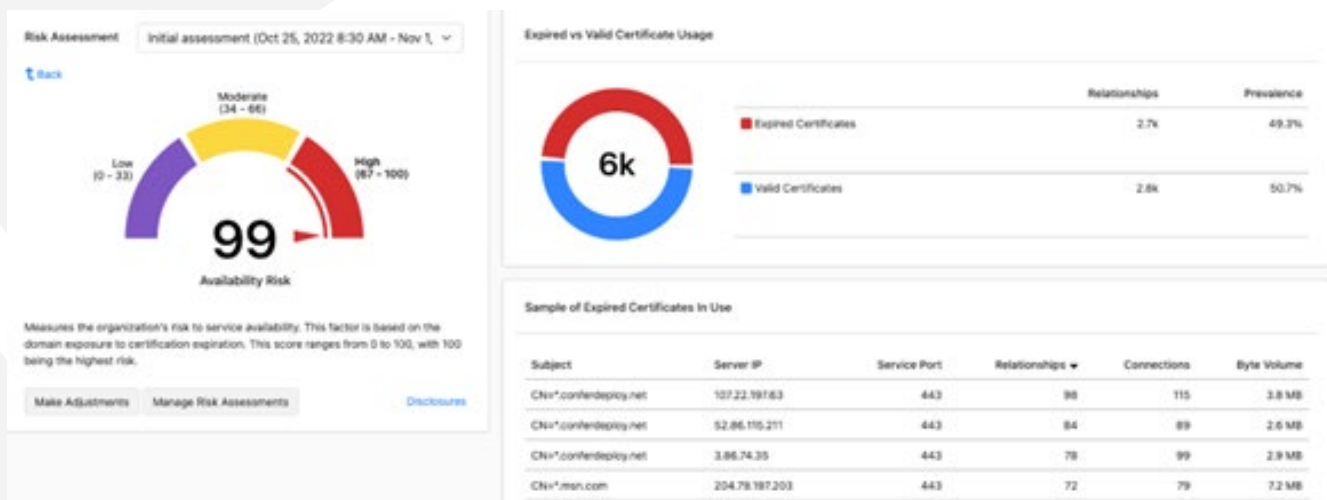
The Application Risk score evaluates availability and security of the cyber environment.



The score is made up of the average of the Availability Risk, Third-Party Risk, and SaaS Risk scorers.

Availability Risk

The Availability Risk score evaluates the use of expired certificates in the cyber environment. If an application is properly configured to not allow the use of expired certificates, then that application will shut down when the server certificate expires.



Third-Party Risk

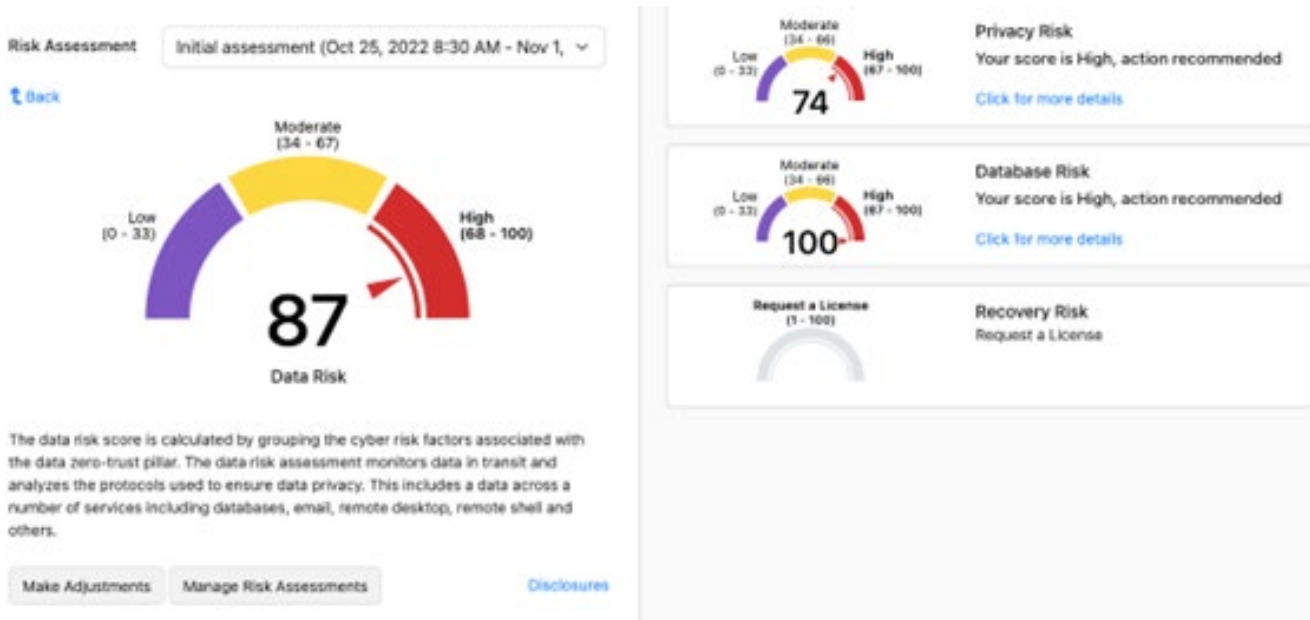
The Third-Party scorer is still under development at this time and is not used in risk scoring at this time.

SaaS Risk

The SaaS Risk scorer is still under development at this time and is not used in risk scoring at this time.

2.3.5 Data Risk

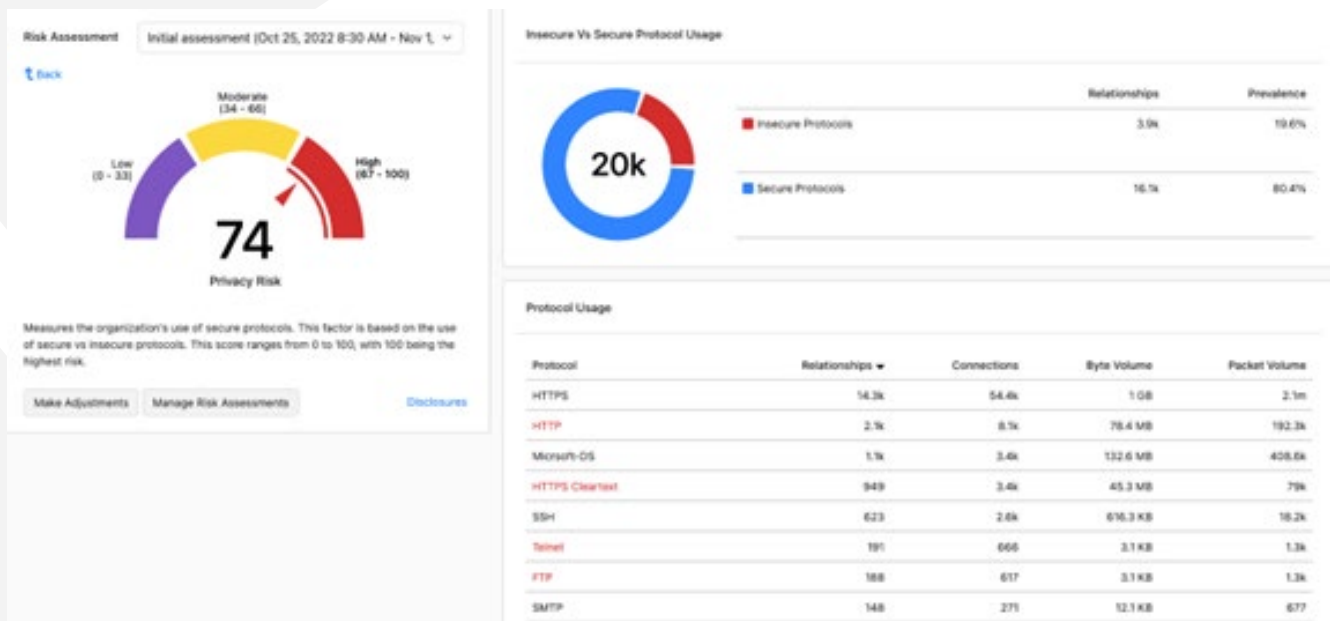
The Data Risk score evaluates the method and security of the flow of data in the cyber environment.



The score is made up of the average of the Privacy, Database, and Recovery Risk scores.

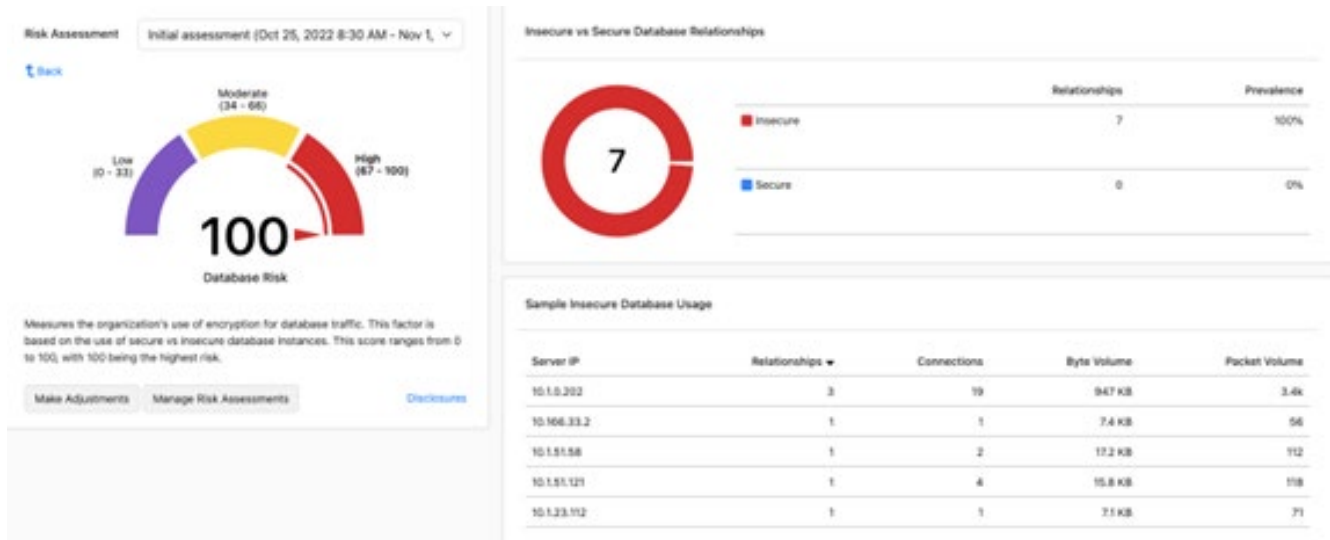
Privacy Risk

The Privacy Risk scorer evaluates the protocols used to move data throughout the cyber environment.



Database Risk

The database risk evaluates the database traffic to determine if that traffic is encrypted.



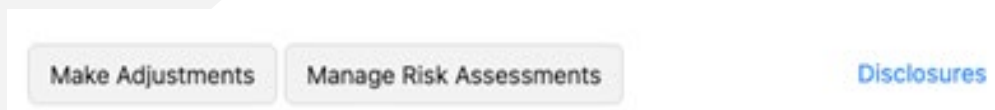
Recovery Risk

The Recovery Risk scorer is still under development at this time and is not used in risk scoring at this time.

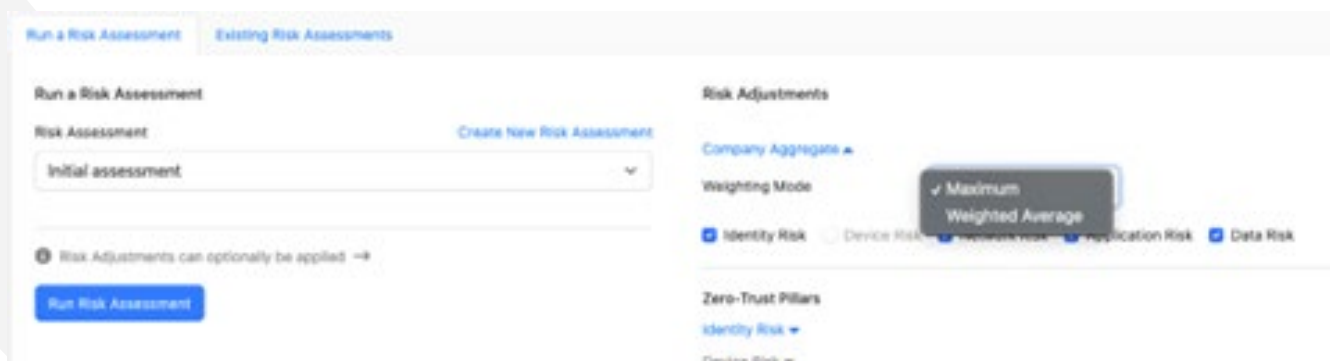
2.4 Risk Adjustments

Once the initial risk assessment has been run and you have evaluated the results, you may choose to adjust the overall or individual scores. You can either make an adjustment to the existing scorer or create a new assessment and adjust prior to running it.

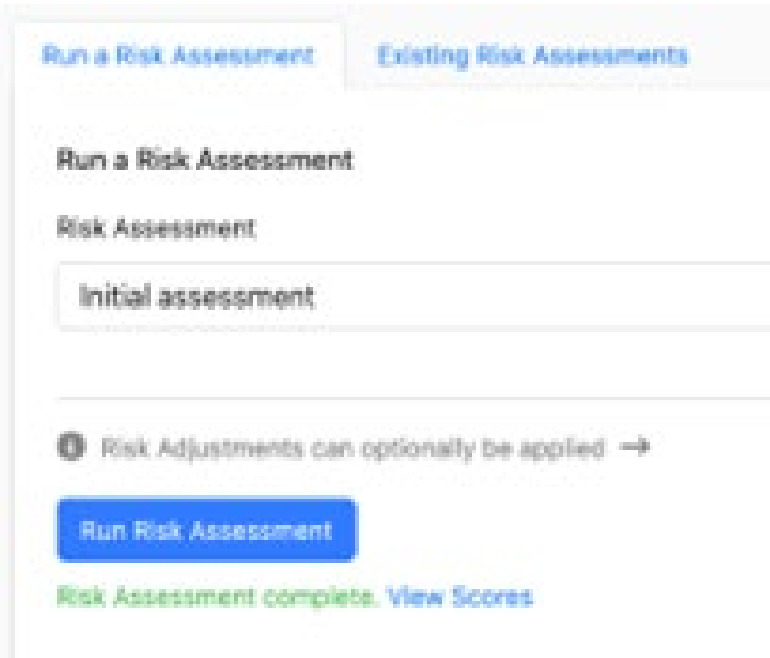
To adjust an existing assessment, click the Make Adjustments button at the bottom of the Company Aggregate pane:



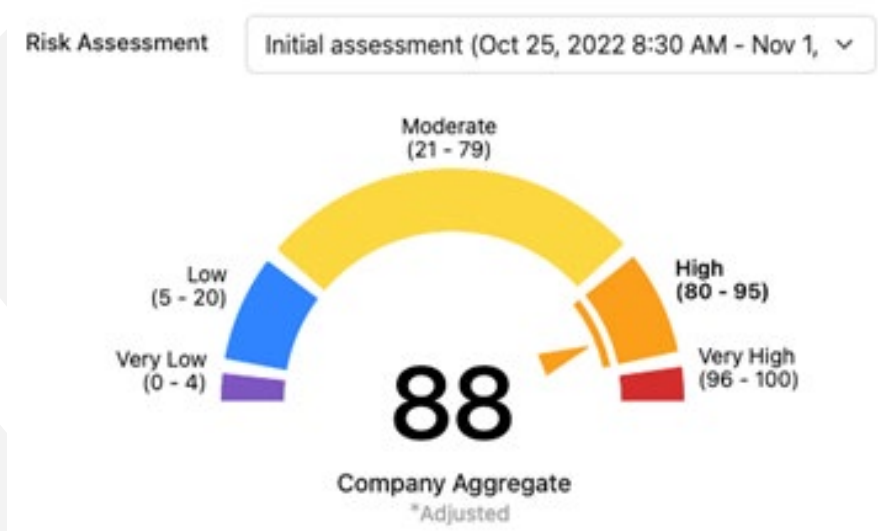
You can adjust any assessment that has already been run. Select the assessment and then make adjustments on the right side of the screen. For example, we can see the same assessment but with weighted average of all scores for the company aggregate rather than the maximum value:



Select Weighted Average and Run Risk Assessment. When the assessment is complete, you will get a message and a button to view the adjusted scores:

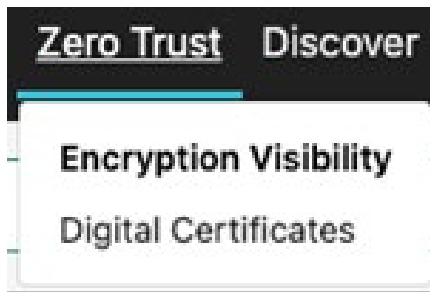


In this example, changing the Company Aggregate score to Weighted Average results in an overall score of 88 vs 100.



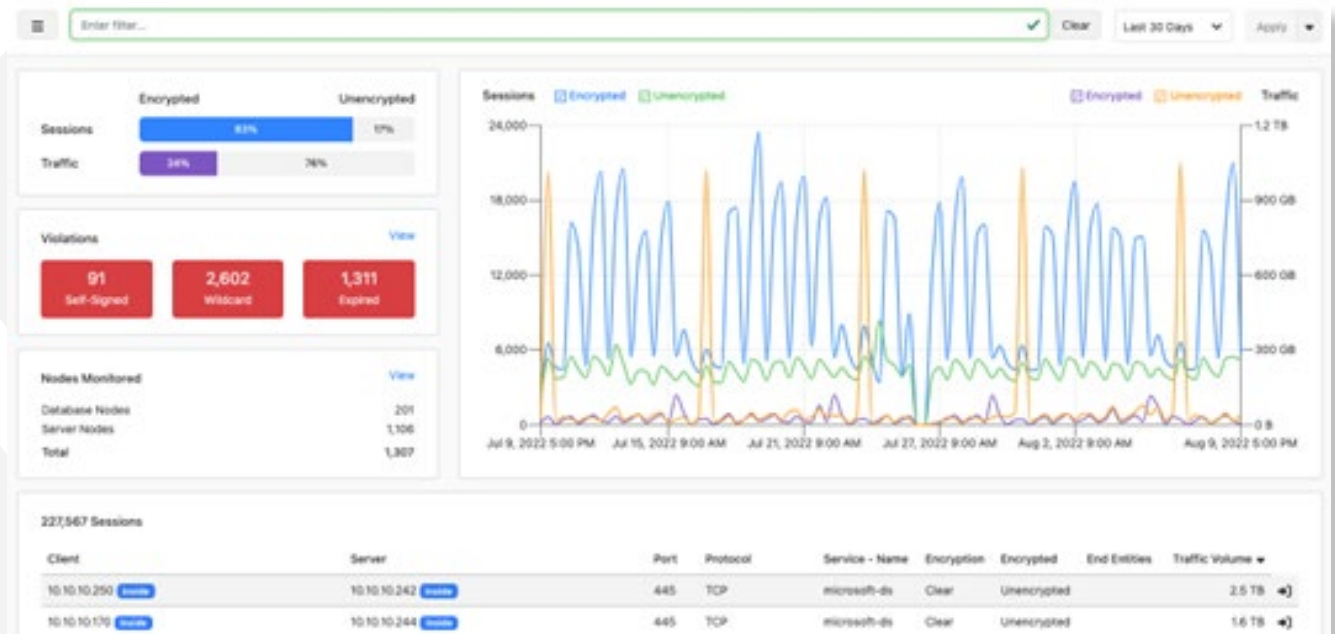
3 Zero Trust

The Zero Trust pages of the CipherInsights product provide dashboard views into the nature of network traffic with respect to encryption and digital certificates. In addition to collecting and evaluating session, traffic, and node data the system evaluates digital certificates and will alert on possible violations such as untrusted, self-signed, or wild card certificates, and definite violations in the form of expired certificates. The Zero Trust tab has two dashboard pages.



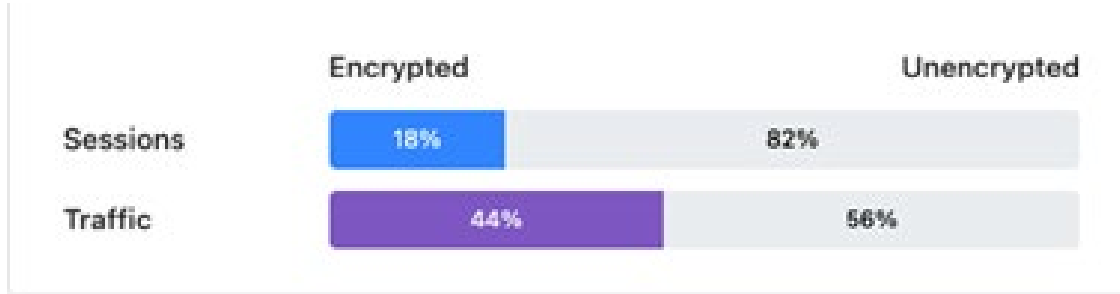
3.1 Encryption Visibility

The Zero Trust Encryption Visibility dashboard provides a summary view of the encryption, certificates, and sessions collected by the CipherInsights software.



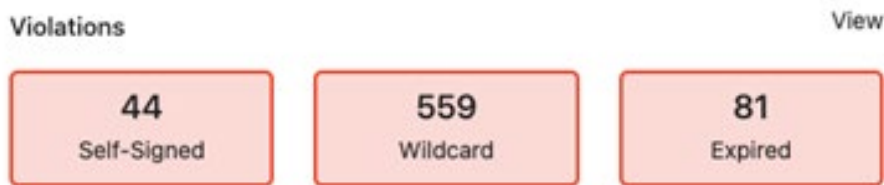
3.1.1 Dashboard Details

On the top left of the screen, the system provides a view into the encryption in motion implemented in the network based on sessions and traffic.



Hovering over and clicking either the Session or Traffic bar graph and clicking the encrypted or unencrypted portion will filter the entire page with the associated information.

The Violations modal provides summary information on certificate issues.



Clicking the View button takes you to the Discover page and displays the pre-defined Violations detailed report. Clicking any individual option, such as "Self-Signed," takes you to the same page and automatically enters the appropriate filter.

```
i certSelfSigned = 'true'
```

The Nodes Monitored modal provides information on both database and server nodes. Clicking the View button takes you to the Discover page and displays the pre-defined Nodes detailed report. Clicking on either Database Nodes or Server Nodes will take you to the Nodes report with the associated filter automatically configured.

Nodes Monitored	View
Database Nodes	315
Server Nodes	12,752
Total	13,067

Detailed session information is displayed at the bottom of the screen in tabular form, based on the selections entered in the search criteria.

691,180 Sessions

Client Domain Name	Client IP	Server Domain Name	Server IP	Server Port	Protocol	Service Name	Encryption	End Entities	Service First Seen	Traffic Volume	Encrypted
	192.168.1.144		10.199.201.68	1433	TCP	ms-sql-s	Clear		Jun 1, 2022 12:48 PM	6.9 GB	Unencrypted
	10.3.24.57		10.199.110.219	1521	TCP	Oracle Database	Clear		Jun 1, 2022 12:50 PM	5.2 GB	Unencrypted
	10.199.110.219		10.3.24.57	1521	TCP	Oracle Database	Clear		Jun 1, 2022 12:50 PM	4.4 GB	Unencrypted
	10.199.100.4		10.199.185.25	2048	TCP	rtf	Clear		Jun 1, 2022 12:56 PM	3.8 GB	Unencrypted
	172.16.100.21		10.99.10.21	5785	TCP	file-caddy	Clear		Jun 1, 2022 12:50 PM	3.4 GB	Unencrypted
	10.19.73.194		10.199.100.8	1528	TCP		Clear		Jun 1, 2022 12:55 PM	2.9 GB	Unencrypted
	10.199.185.25	k3-us-east-1-r-w.amazonaws.com	52.216.3.13	443	TCP	https	TLS	1	Jun 1, 2022 12:48 PM	2.8 GB	Encrypted
	10.199.206.17		10.199.40.10	4306	TCP		TLS		Jun 1, 2022 12:55 PM	2.5 GB	Encrypted
	10.0.255.29		10.80.15.64	5985	TCP	woman	Clear		Jun 1, 2022 12:50 PM	2.1 GB	Unencrypted

This data can be sorted by any of the columns in the display. The initial click will sort from lowest to highest, a second click reverses the order.

3.2 Digital Certificates

The Digital Certificates function of the product provides detailed information about certificate usage throughout the network. This includes total end-entities and flags for self-signed, wild card, and expired certificates. In addition, the page summarizes the number of certificates in use by Certificate Authorities and the encryption version used for each. The page can be filtered as described previously.

3.2.1 Dashboard Details

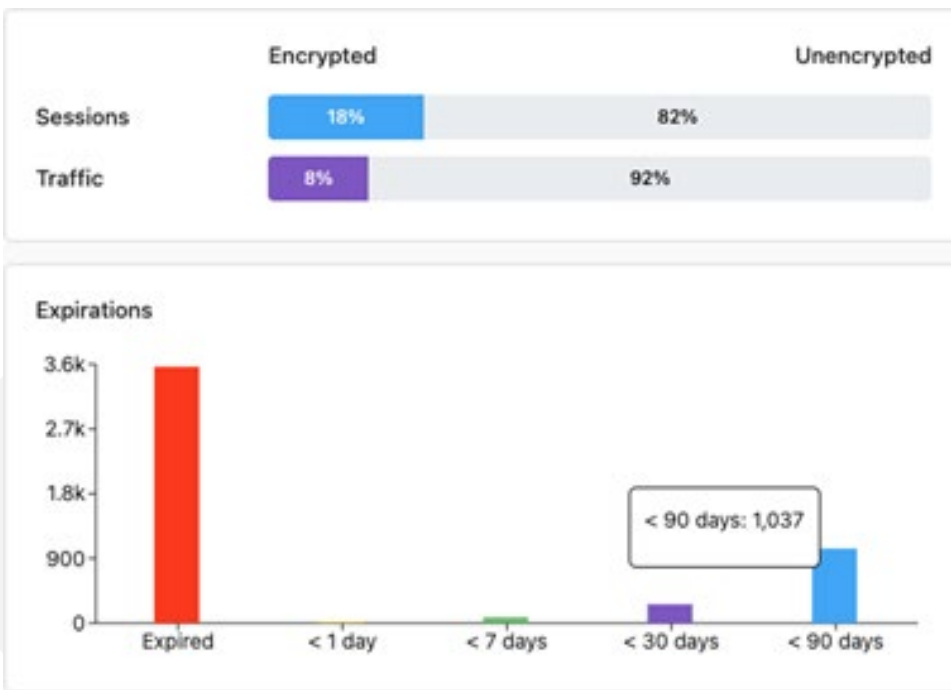
The overview page provides a summary of certificate and session information collected by the system, including encryption version information, certificate expirations, and certificate authorities along with detailed information on each certificate chain in tabular form at the bottom of the page.



The Certificate Authorities modal can be displayed either by connection count or client count. Selecting the “more” count at the bottom of the page takes you to the Discover page and displays the Certificate Authority report which displays all certificate authorities captured by the system.

122 Certificate Authorities		
Issuer - Organization	Client Count	New Connections
ACME	1321	81,076
acme-mbs1.2462nc	16	344,078
AddTrust AB	11	99
AffinityTrust	1	3
Amazon	371	4,472
American Power Conversion Corp	2	21

The center portion of the display includes the encryption summary graph and a bar graph of certificate expirations.



Clicking any of the bars in the Expirations graph takes you to the Discover page and displays the certificate page, filtered according to the graph you select.

The bottom of the page includes a list of certificate chains identified by the application, sorted by traffic volume.

367 Certificate Chains							
Subject - Common Name	Issuer - Organization	Not Valid After	All Names	Signature Algorithm	Servers	New Connections	Traffic Volume
intigua-server	Intigua Inc.	Jun 22, 2031 9:09 AM	(8)	sha256WithRSAEncryption	(1)	5.8k	121.5 MB
*conferdeploy.net	GoDaddy.com, Inc.	Aug 29, 2022 11:35 AM	(8)	sha256WithRSAEncryption	(78)	2.4k	72.9 MB
video.csod.com	DigCert Inc	Apr 7, 2023 6:59 PM	(8)	sha256WithRSAEncryption	(1)	4	38.9 MB
www.bing.com	Microsoft Corporation	Dec 8, 2022 7:15 PM	(28)	sha256WithRSAEncryption	(8)	112	28.7 MB

Selecting an individual certificate from the list, by using the arrow button on the right side of the row, will take you to the Certificate detail page. The system will provide an overview of the certificate, including Subject, Issuer, Root CA, and Expiration. It also includes the Validation status and offers the user the ability to look at the detailed certificate, text, and the mesh of the certificate chain.


Certificate Chain - *.conferdeploy.net

Overview

Subject - Common Name: *.conferdeploy.net
 Issuer - Organization: GoDaddy.com, Inc.
 Root CA - Organization: GoDaddy.com, Inc.
 Expires: August 29, 2022 9:35 AM (PDT)

Number of servers: 76
 Number of clients: 609

Certificate Chain Explorer



***.conferdeploy.net**
 Issued by: GoDaddy.com, Inc.
 Expires: August 29, 2022 9:35 AM (PDT)

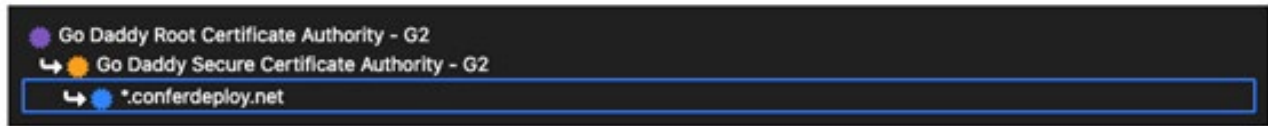
[Details](#) [Text](#) [Mesh](#)

Validation ● Failed Validation

Last validated on: October 31, 2022 8:43 AM (PDT)

- This certificate chain has expired

Certificate Chain Explorer



***.conferdeploy.net**
 Issued by: GoDaddy.com, Inc.
 Expires: August 29, 2022 9:35 AM (PDT)

[Details](#) [Text](#) [Mesh](#)

Certificate:

Data:

```

Version: 3 (0x2)
Serial Number: 3301707177617479321 (0x2dd2052f523f5699)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com, In
Validity
  Not Before: Jul 28 16:35:53 2021 GMT
  Not After : Aug 29 16:35:53 2022 GMT
Subject: CN=*.conferdeploy.net
Subject Public Key Info:
  
```



Certificate Chain Explorer

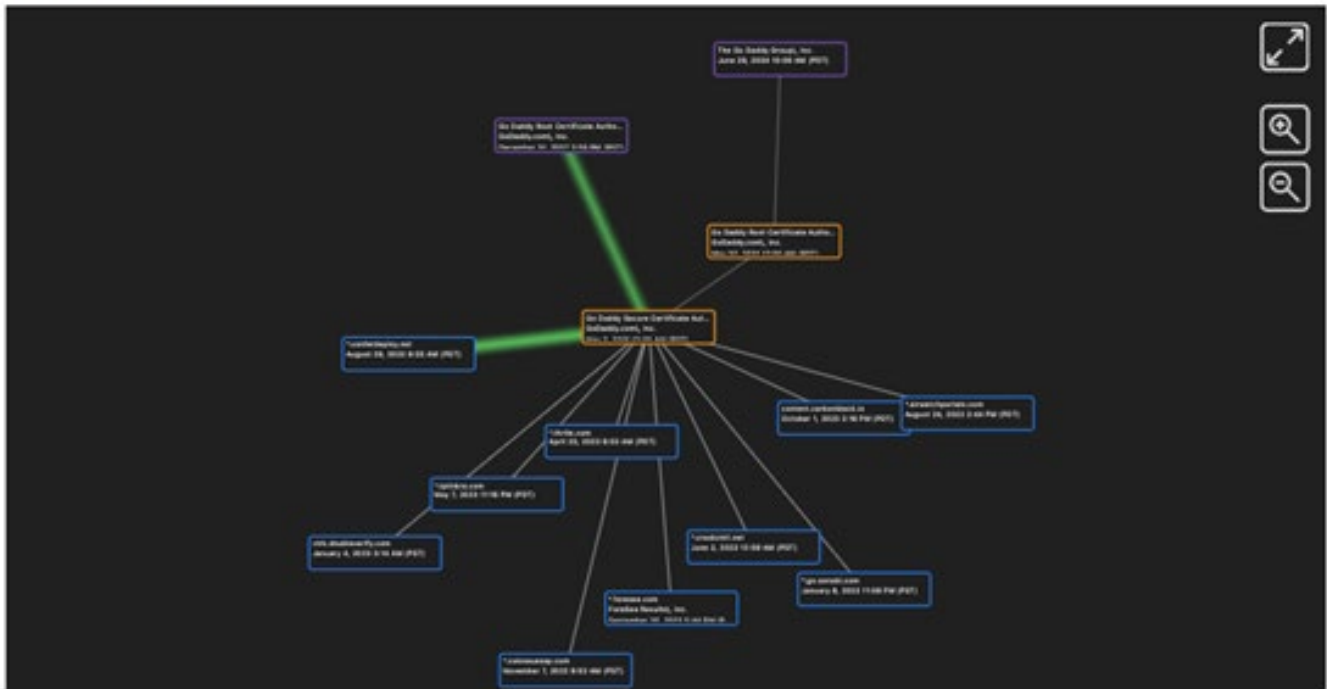
- Go Daddy Root Certificate Authority - G2
- Go Daddy Secure Certificate Authority - G2
- *.conferdeploy.net**



***.conferdeploy.net**

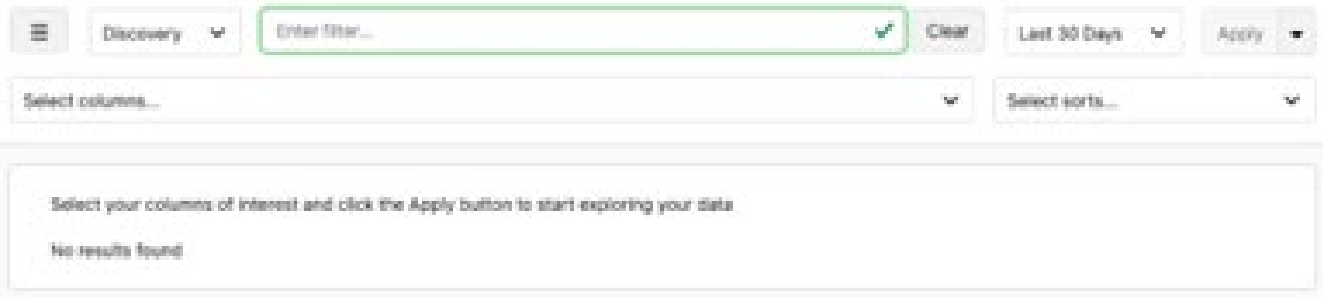
Issued by: GoDaddy.com!, Inc.
Expires: August 29, 2022 9:35 AM (PDT)


Details ▾ Text ▾ Mesh ▲

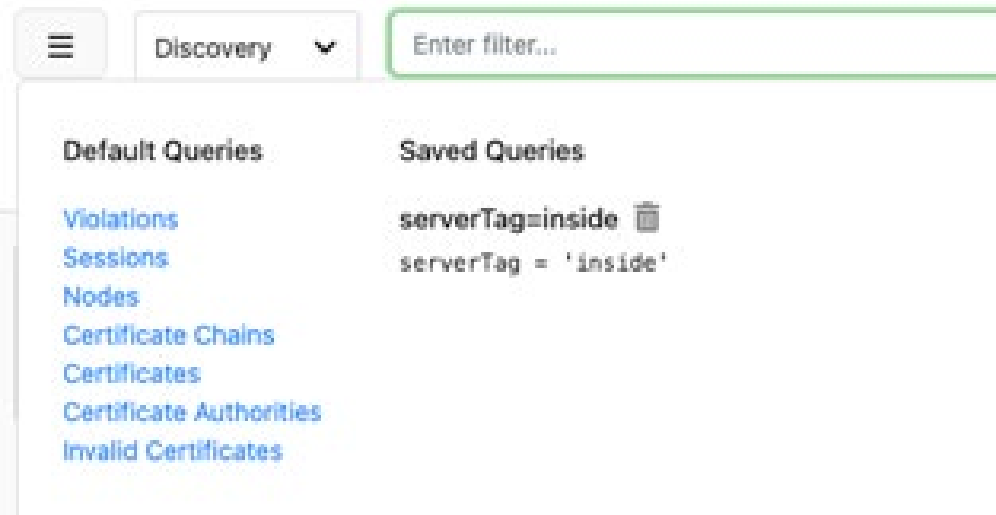


4 Discover

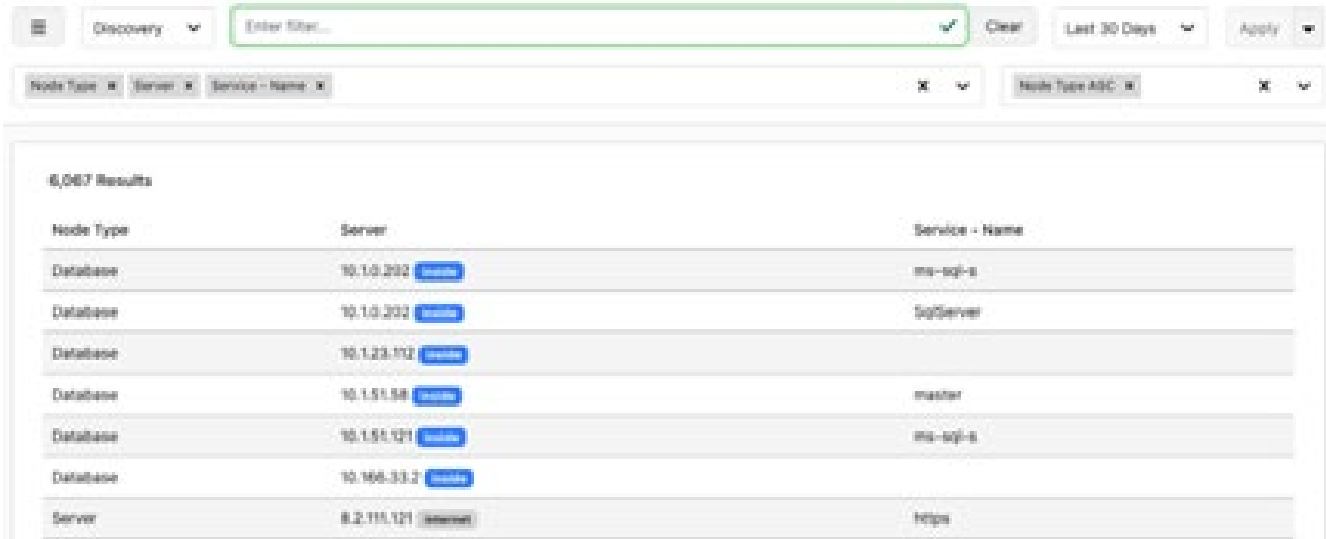
The Discover tab provides a rich search engine that allows you to query the system data lake and build reports derived from all the data the system collects. The language is SQL-like, but specific to the CipherInsights system.



The system provides a pre-configured set of reports that can be viewed by clicking the saved search button  on the left side of the filter line. These reports are described later in this section.



Selecting one of the reports will provide an example of the language used to develop that report. For example, the Nodes report will display:



Node Type	Server	Service - Name
Database	10.1.0.202 inside	ms-sql-s
Database	10.1.0.202 inside	SqlServer
Database	10.1.23.112 inside	
Database	10.1.51.58 inside	master
Database	10.1.51.121 inside	ms-sql-s
Database	10.168.33.2 inside	
Server	8.2.111.121 server	https

The items included in the report are shown at the top of the page.



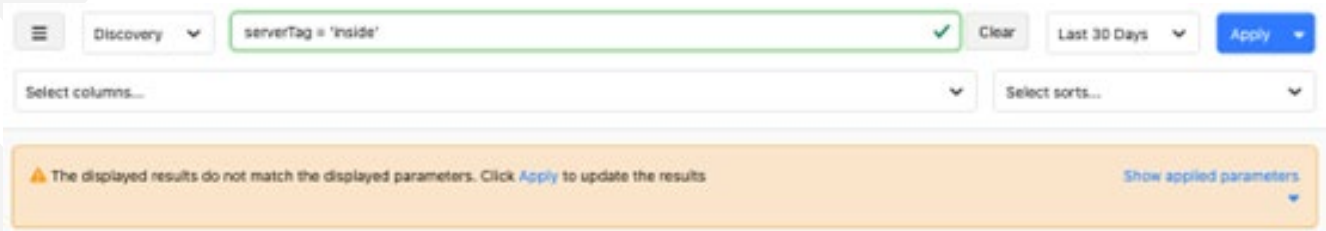
nodeType	serverName	serverip	serviceName	serviceFirstSeenEpoch	serverHostid	leftJoinServerTagsGivenServerHostid
----------	------------	----------	-------------	-----------------------	--------------	-------------------------------------

The box on the right is the sort order. If a field is sortable, it will be displayed in the drop-down box.



serviceFirstSeenEpoch DESC


You can limit the amount of data in the report by using the filter bar at the top, and you can select previously saved queries to filter the data. As in the case of other screens, the filter must be applied to adjust the results of the displayed report.

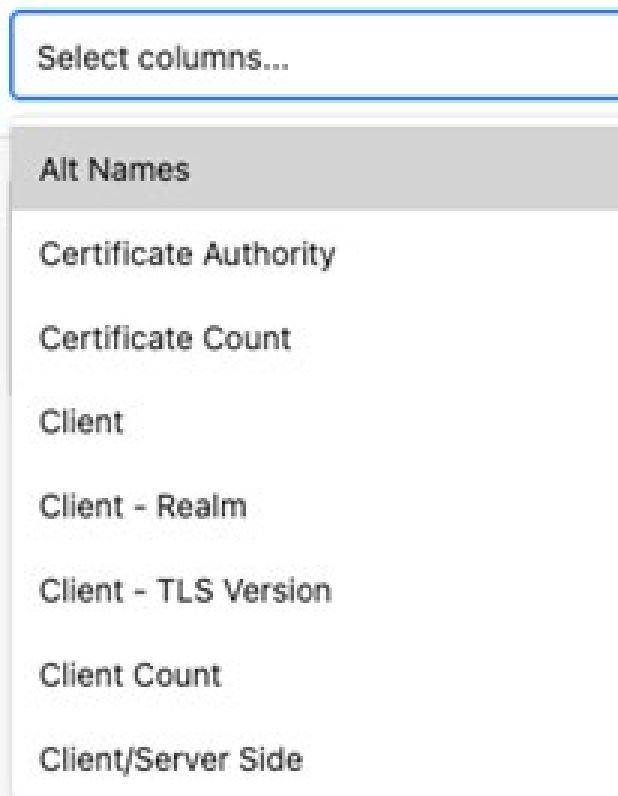


Discovery Clear Last 30 Days Apply

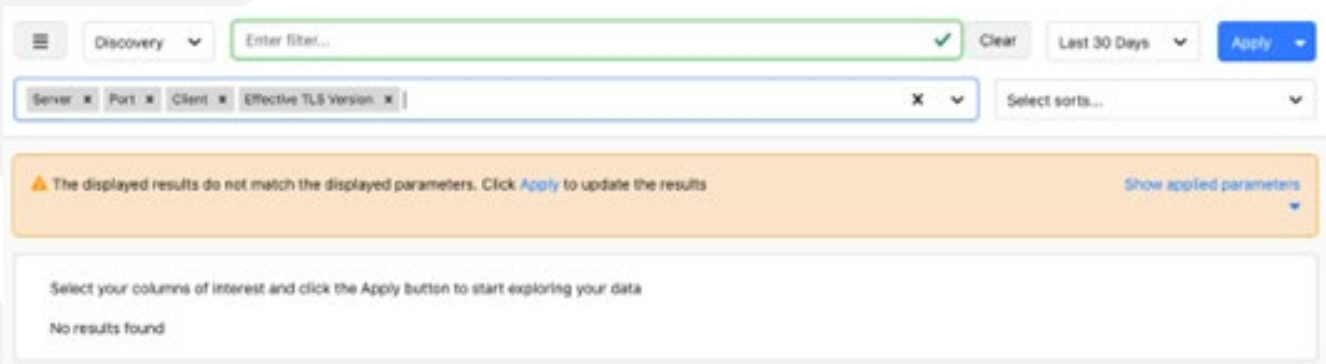
Select columns... Select sorts...

Warning: The displayed results do not match the displayed parameters. Click [Apply](#) to update the results. [Show applied parameters](#)

You can use the drop-down button  to build a new report. When you click that button the list of options is displayed. Click on an item to include it in the report.



When the items selected and filter are correct, the system will prompt you to click Apply to execute the report.



The system allows you to create a report from a properly formatted discovery search for use later in the Reports page. Select the Apply button on the top right of the screen and then select Save Query to open the report creation tool.

Save Query and Create Report ✕

Name

Create Report?

Save Query and Create Report ✕

Name

Create Report?

Plugin

 ▼

Description

Run nightly

Report title

Unique component of output filename

DTA command

 ▼

DTA arguments

The Description will be used on the reports page as the name of the report. The Report Title is displayed on the report when run. The string entered in the Unique component output file name field will be added to the report each time it is run and is important when multiple reports will be run and downloaded on the same day. The name must not contain spaces or special characters other than dash (-) or underscore (_).

Check the appropriate box for pdf and/or csv file generation. To get the complete report in pdf, set the Maximum rows to show in pdf report to zero. The system limits PDF reports to a maximum of 500 rows of data.

Each report created in the Discover page will be available in the Reports > DTA Report page, described in Section 6.

Items that can be grouped for display are listed in Table 4-1.

Table 4-1. Validation Fields

Field	Description	Options/Format
Alt Names	Indicates the number and detail of alt names found in the certificate	Number/text
Certificate Authority	Indicates if the certificate authority is in the trust store	True/false
Certificate Count	Number of certificates identified in a certificate chain	Number
Client	IP address and domain name (if available via DNS lookup) of the client in the session	0.0.0.0
Client Realm	The client realm, if configured	Text
Client – TLS Version	Version of TLS supported by the client	Text
Client Count	Number of clients associated with the reported object	Number
Client/Server Side	Identifies if a node has been identified as a client or server	Client/server
Dialect	The database dialect, when applicable. SQL Server, Oracle	Text
Effective TLS Version	Version of TLS negotiated on the session	Text
Encrypted	Whether or not encryption is detected in the session	True/False
Encryption	Identifies the type of encryption used in the session, if applicable.	Clear or Encryption Type
End Entities	Identifies the service or URL identified, if applicable	Text
Ended Connections	Number of connections that completed	Number
First Seen	Date and timestamp when a service or database is first detected by the system	Date/Time
Issuer	The issuing company for the certificate	Text
Issuer - Organization	The issuing company for the certificate	Text
Last Seen	Identifies the last date/time traffic was seen for the object in the report	Date/Time
New Connections	A count of new connections seen for the time window selected	Number
Node Type	Type of Node	Server/Database
Not Valid After	Date the certificate is not valid after	Date/Time
Not Valid Before	Date the certificate is not valid before	Date/Time
Packet Volume	Number of total packets seen for the object in the report	Number

Field	Description	Options/Format
Packets to Client	Number of packets destined for the client that were seen for the object in the report	Number
Packets to Server	Number of packets destined for the server that were seen for the object in the report	Number
PEM	The PEM of the certificate	Text
Port	The port used by the client and/or server in the session	Number
Protocol	The communication protocol detected in the conversation	Text
Proxy	Indicates if the certificate is configured as a proxy	True/false
Public Key	The public key of the certificate	Text
Public Key Algorithm	The public key algorithm of the certificate	Text
Self-Signed	Indicates if the certificate is self-signed	True/false
Serial Number	Certificate serial number	Number
Server	IP address and domain name (if available via DNS lookup) of the server in the session	0.0.0.0
Server Certificates	Includes the server certificates detected in the session	Text
Server Realm	The server realm, if configured	Text
Servers	When used on a certificate report, identifies the servers using the associated certificate	Number/text
Service - Name	Service name of the database or application, if applicable	Text
Signature	The signature portion of the certificate	Text
Signature Algorithm	The signature algorithm of the certificate	Text
Subject	The subject information of the certificate	Text
Subject – Common Name	The CN of the certificate	Text
Text	The complete certificate text	Text
Traffic Volume	Number of total bytes seen for the object in the report	Number
Traffic Volume to Client	Number of bytes destined for the client that were seen for the object in the report	Number
Traffic Volume to Server	Number of bytes destined for the server that were seen for the object in the report	Number
Trust	The trust status of the certificate in the system	Infer/Never/Always
Valid	Indicates if the certificate is valid	True/false
Validated On	Date/time the certificate was validated	Date/time
Validations	Text describing validation issues, if applicable	Text
Version	Certificate version	Number
Wildcard	Indicates if the certificate uses a wildcard	True/false

4.1 Violations

The Violations page provides a tabular list of all sessions in which certificate violations were detected. The display includes the number of connections and traffic volume. This data can be sorted by any of the columns in the display. The initial click will sort from lowest to highest, a second click reverses the order.

Subject - Common Name	Issuer - Organization	Not Valid After	All Names	Signature Algorithm	Servers	New Connections	Byte Volume
gspolbed04	CommVault Systems, Inc.	Aug 3, 2021 4:58 AM	2	sha256WithRSAEncryption	2	2	185.5 GB
*s.acome-ad.com		Apr 20, 2023 10:28 AM	2	sha256WithRSAEncryption	22	19,722,298	88.8 GB
gspolbed01	CommVault Systems, Inc.	Aug 4, 2021 1:40 AM	2	sha256WithRSAEncryption	2	7	70.3 GB
mesa16.s.acome-ad.com	kapaku.s.acome-ad.com	Jul 7, 2021 8:59 AM	2	sha256WithRSAEncryption	2	20,405	59.9 GB
SolarWinds-Orion		Dec 31, 2039 3:59 PM	2	sha256WithRSA	2	180,795	54.6 GB
mesa17.s.acome-ad.com	kapaku.s.acome-ad.com	Jul 7, 2021 8:59 AM	2	sha256WithRSAEncryption	2	20,749	49.2 GB
gspolbed01	CommVault Systems, Inc.	Aug 3, 2021 3:45 AM	2	sha256WithRSAEncryption	2	1	27.2 GB
mesa07.s.acome-ad.com	kapaku.s.acome-ad.com	Jun 30, 2021 3:10 PM	2	sha256WithRSAEncryption	2	20,494	21.6 GB
SMS-160418195817684	VMware	Apr 18, 2026 12:58 PM	2	sha256WithRSAEncryption	22	2,458,868	15.4 GB

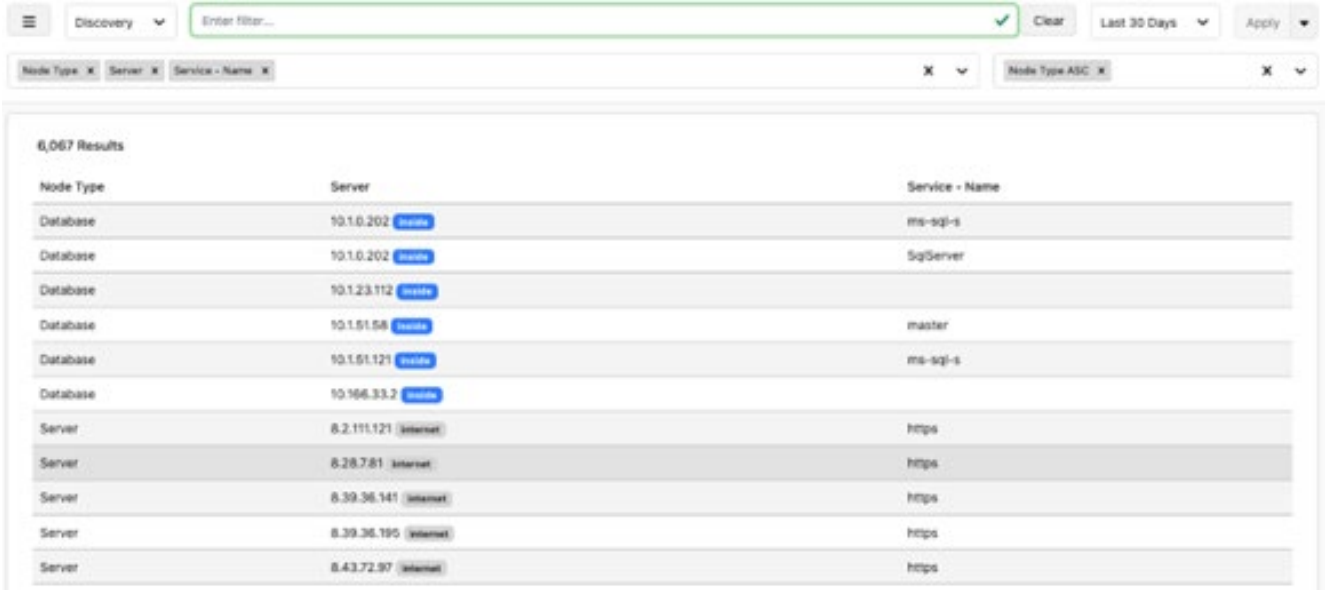
4.2 Sessions

The Sessions page displays the complete detail for each session detected in tabular form. This includes both encrypted and unencrypted sessions. The search criteria line can be used to narrow the display, and the data can be sorted by any of the columns in the display. The initial click will sort from lowest to highest, a second click reverses the order.

Client Domain Name	Client IP	Client Host ID	Server Domain Name	Server IP	Server Host ID	Server Port	Protocol	Service Name	Service Nam
	192.168.1.144	4531		10.199.201.66	4530	1433	TCP	ms-sql-s	false
	10.3.24.57	4653		10.199.110.219	4511	1521	TCP	ncube-lm	false
	10.199.100.6	4586		10.199.185.25	4553	2049	TCP	Oracle Database	false
	10.199.110.219	4511		10.3.24.57	4653	many	TCP	Oracle Database	false
	10.19.73.194	36826		10.199.100.6	4586	1528	TCP		false

4.3 Nodes

The Nodes page displays information on the nodes discovered by the product. The page can be filtered by time and search criteria, like prior pages. The table can be sorted by any column displayed on the page.



Discovery Clear Last 30 Days Apply

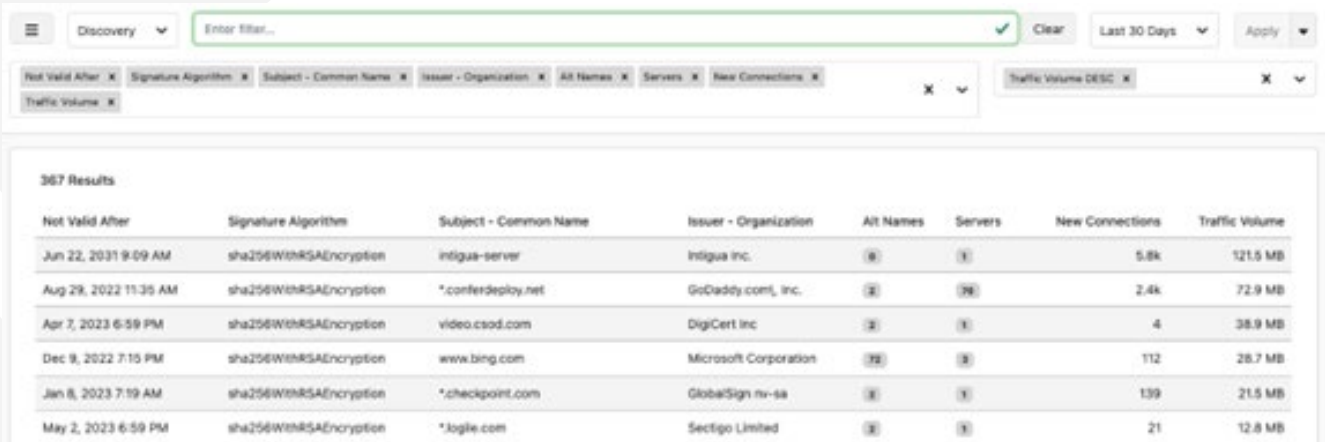
Node Type X Server X Service - Name X Node Type ASC X

6,067 Results

Node Type	Server	Service - Name
Database	10.1.0.202 Nodes	ms-sql-s
Database	10.1.0.202 Nodes	SqServer
Database	10.1.23.112 Nodes	
Database	10.1.51.58 Nodes	master
Database	10.1.51.121 Nodes	ms-sql-s
Database	10.166.33.2 Nodes	
Server	8.2.111.121 Internet	https
Server	8.28.7.81 Internet	https
Server	8.39.36.141 Internet	https
Server	8.39.36.195 Internet	https
Server	8.43.72.97 Internet	https

4.4 Certificate Chains

The Certificate Chains page provides a list of all certificate chains identified by the system. The page includes the subject common name, issuer organization, validation end data, the signature algorithm that determines TLS level, the number servers identified as using the certificate, number of connections, and amount of traffic seen with that certificate chain.



Discovery Clear Last 30 Days Apply

Not Valid After X Signature Algorithm X Subject - Common Name X Issuer - Organization X All Names X Servers X New Connections X Traffic Volume X Traffic Volume DESC X

367 Results

Not Valid After	Signature Algorithm	Subject - Common Name	Issuer - Organization	All Names	Servers	New Connections	Traffic Volume
Jun 22, 2031 9:09 AM	sha256WithRSAEncryption	intigua-server	Intigua Inc.	(8)	(1)	5.8k	121.5 MB
Aug 29, 2022 11:35 AM	sha256WithRSAEncryption	*confereDeploy.net	GoDaddy.com, Inc.	(3)	(76)	2.4k	72.9 MB
Apr 7, 2023 6:59 PM	sha256WithRSAEncryption	video.csod.com	DigCert Inc	(3)	(1)	4	38.9 MB
Dec 9, 2022 7:10 PM	sha256WithRSAEncryption	www.bing.com	Microsoft Corporation	(7)	(3)	112	26.7 MB
Jan 8, 2023 7:19 AM	sha256WithRSAEncryption	*checkpoint.com	GlobalSign nv-sa	(1)	(1)	139	21.5 MB
May 2, 2023 6:59 PM	sha256WithRSAEncryption	*logile.com	Sectigo Limited	(3)	(1)	21	12.8 MB

4.5 Certificates

The Certificates page provides a tabular list of all certificates detected by the system. The data can be filtered using the search bar and the amount of data can be adjusted based on the date, in the same manner as other pages. The data can be sorted by clicking on the associated column.

The screenshot shows the Certificates page interface. At the top, there is a search bar with the placeholder text "Enter filter...". To the right of the search bar are buttons for "Clear", "Last 30 Days", and "Apply". Below the search bar is a row of filter options: "Subject", "Issuer", "Not Valid Before", "Not Valid After", "Version", "Self-Signed", "Wildcard", "Certificate Authority", "Text", "PEM", "Trust", and "Traffic Volume". There are also buttons to remove filters (indicated by 'x') and a dropdown arrow. Below the filters is a table with 367 results. The table has columns: Subject, Issuer, Not Valid Before, Not Valid After, Version, Self-Signed, Wildcard, Certificate Authority, View Certificate, View PEM, Trust, and Traff. The first three rows of the table are visible, showing certificates issued by "Cisco Umbrella Secondary SubCA Inc." for the domain "content.govdelivery.com".

The page includes an option to add or remove columns from the page display by editing the options at the top of the page.

This screenshot shows the column selection interface. It features a search bar "Enter filter..." and buttons for "Clear", "Apply", "Save Query", and "CU - Docs". Below the search bar is a list of column names with 'x' icons to remove them: "certId", "certSubject", "certIssuer", "certNotValidBeforeEpoch", "certNotValidAfterEpoch", "certVersion", "certSelfSigned", "certWildcard", "certCa", "certText", "certPem", "certSkid", "certAid", and "certTrust". A dropdown arrow is visible on the right side of the list.

Delete columns by clicking the x next to the item to remove and selecting Apply.

To add columns, use the drop-down arrow on the right side of the list and select the option you wish to display.

This screenshot shows the column selection dropdown menu. The list of columns is: "certAnyEku", "certCnt", "certCodeSign", and "certCriSign". The "certAnyEku" option is currently selected and highlighted in blue.

Certificate details such as subject, issuer, validation dates, subject key identifier, and authority key identifier are displayed. You can click to view the certificate and PEM. The validation status of self-signed, wildcard, and certificate authority are also displayed.

Finally, the current trust status is displayed. If the Trust identifier is "Infer," it is being validated using the system trusted certificate store. You may set the trust status of individual certificates on the Certificate Validation page. See Section 7, Certificate Validation for details.

4.6 Certificate Authorities

The Certificate Authority page provides a tabular list of all certificate authorities identified by the system. The data can be filtered by subnet and the amount of data can be adjusted based on the date, in the same manner as other pages.

All certificate authorities are initially displayed; each column can be used to sort the display.

111 Certificate Authorities

Issuer - Organization	Client Count	New Connections
K Software	1	1
Mercury Security Products	1	1
iPlanet, Inc.	1	1
AdventTrust	1	1
Quintado Limited	2	2
Cisco Systems Inc.	1	2
CyberPower Systems, Inc.	1	2
GoGetSSL	2	3
The USERTRUST Network	1	3
Support	2	4
Flare, Inc.	1	4

4.7 Invalid Certificates

The application evaluates all certificates to determine if they are valid. The Invalid Certificates page provides a tabular view of all certificates that failed validation, the date and time the validation was run, the reason it failed, along with other details about the certificate.

Search: ... Clear Last 14 days

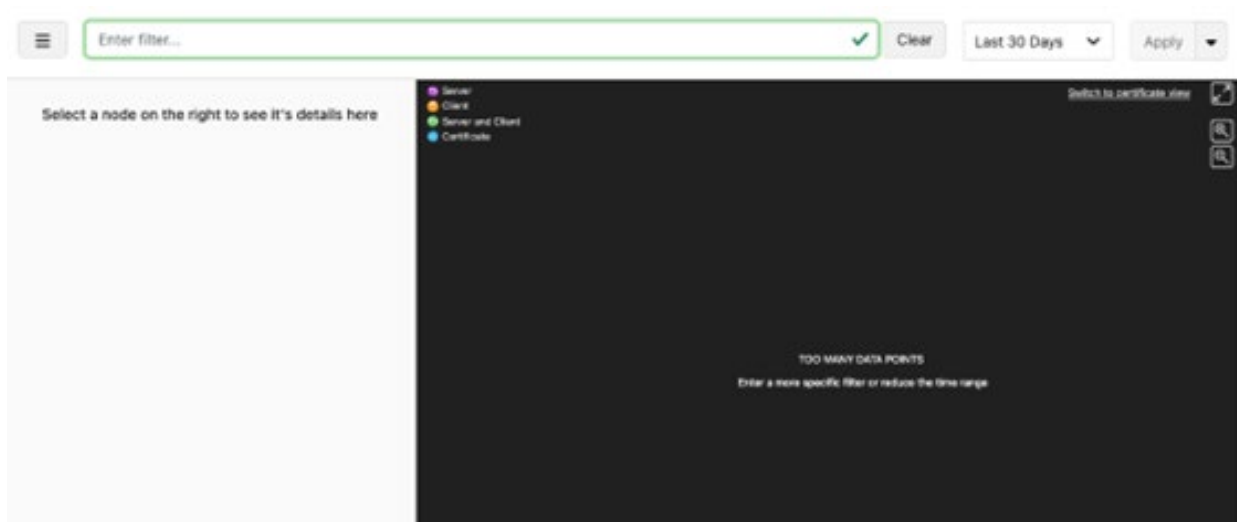
Invalid Certificates


Validated On	Validations	Subject - Common Name	Issuer - Organization	Not Valid After	All Names	Servers	New Connections	Byte Volume
Dec 25, 2021 8:24 AM	The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates	4ec26782-5783-4911-8192-5887952f6d68	Microsoft	Mar 25, 2022 9:24 AM	2	1	16,542	1.9 GB
Dec 25, 2021 8:22 AM	The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates	844a4886-6d79-449e-87f5-56a773e7906	Microsoft	Mar 25, 2022 9:22 AM	2	1	16,917	2.0 GB
Dec 25, 2021 8:19 AM	The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates	300d921-5941-4642-8381-aa79f58a096	Microsoft	Mar 25, 2022 9:19 AM	2	1	16,572	1.9 GB

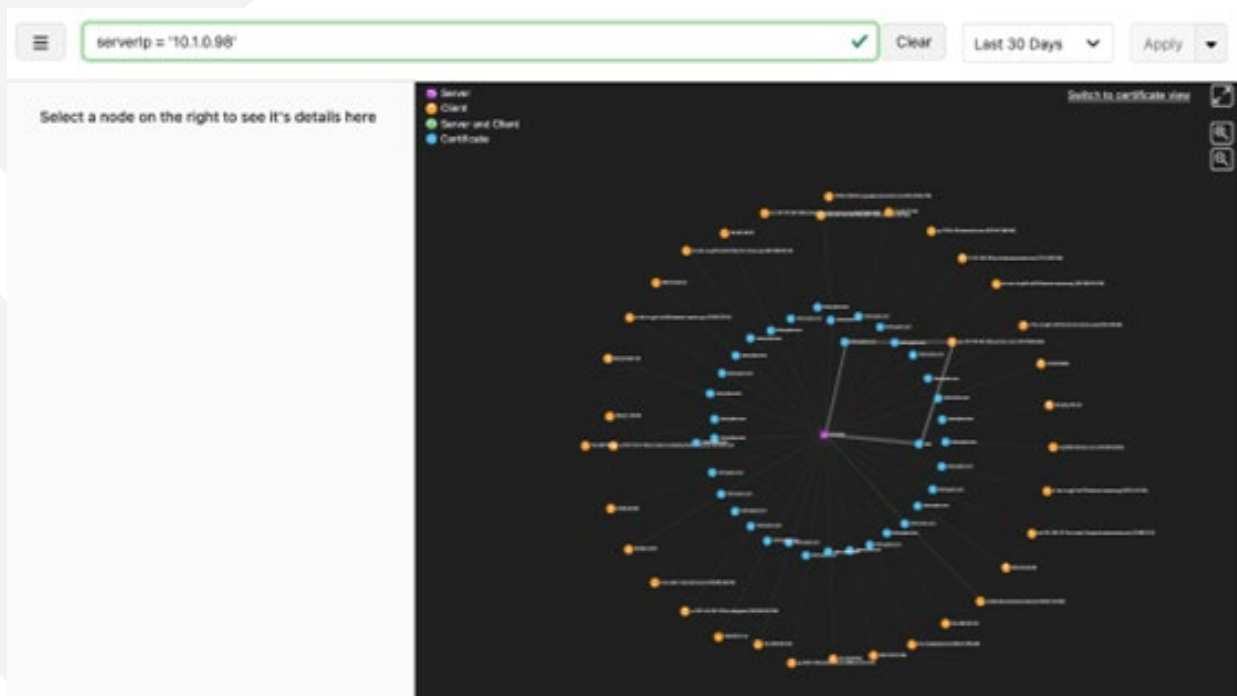
5 Explore

The explore page provides a graphical view of server, client, and certificate interactions. The tool allows a user to map applications and evaluate certificate usage.

Depending on the amount of traffic captured, the system will typically display “Too Many Data Points” if no search criteria is entered.

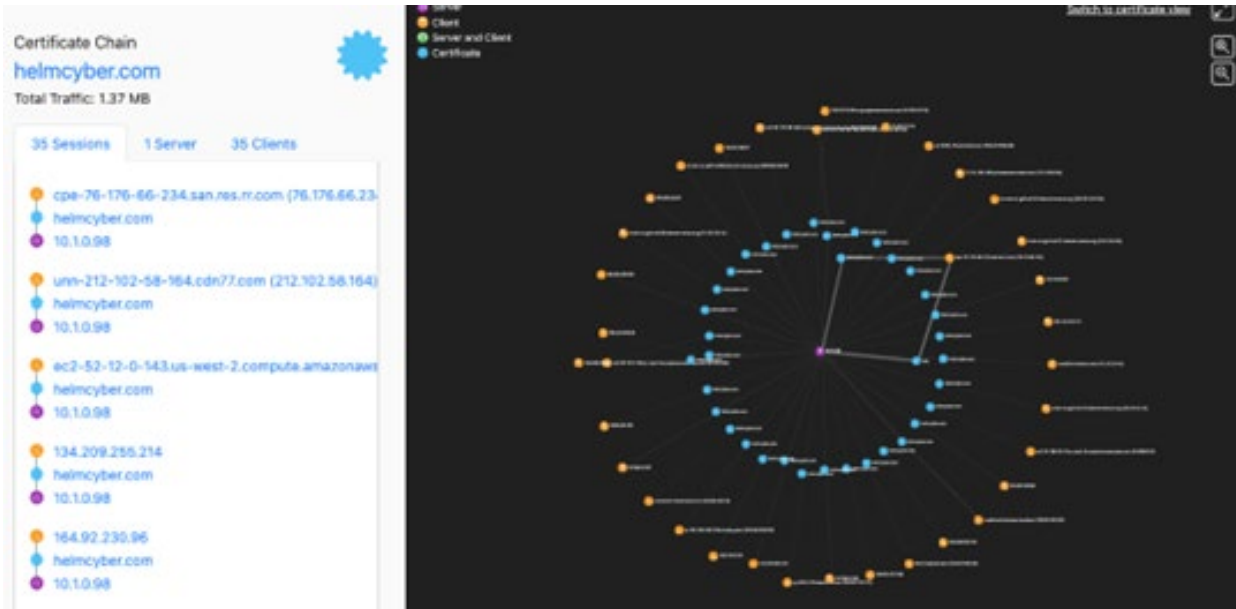


The information  button provides help for entering search criteria, including the format of the command. One simple view is to select a specific server IP to evaluate:

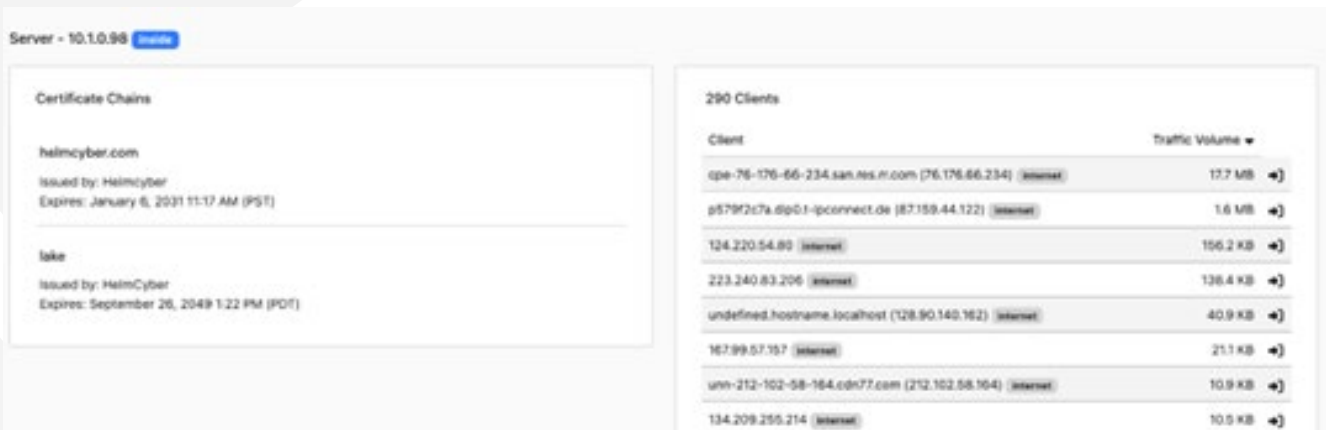


The system defaults to displaying the session view, including servers, clients, and all certificates in use. Clicking on the certificate view button in the top right of the screen will change the display to focus on the display on the interactivity of the certificate.

Clicking on each of the datapoints in the graph will display detailed information about that entity.



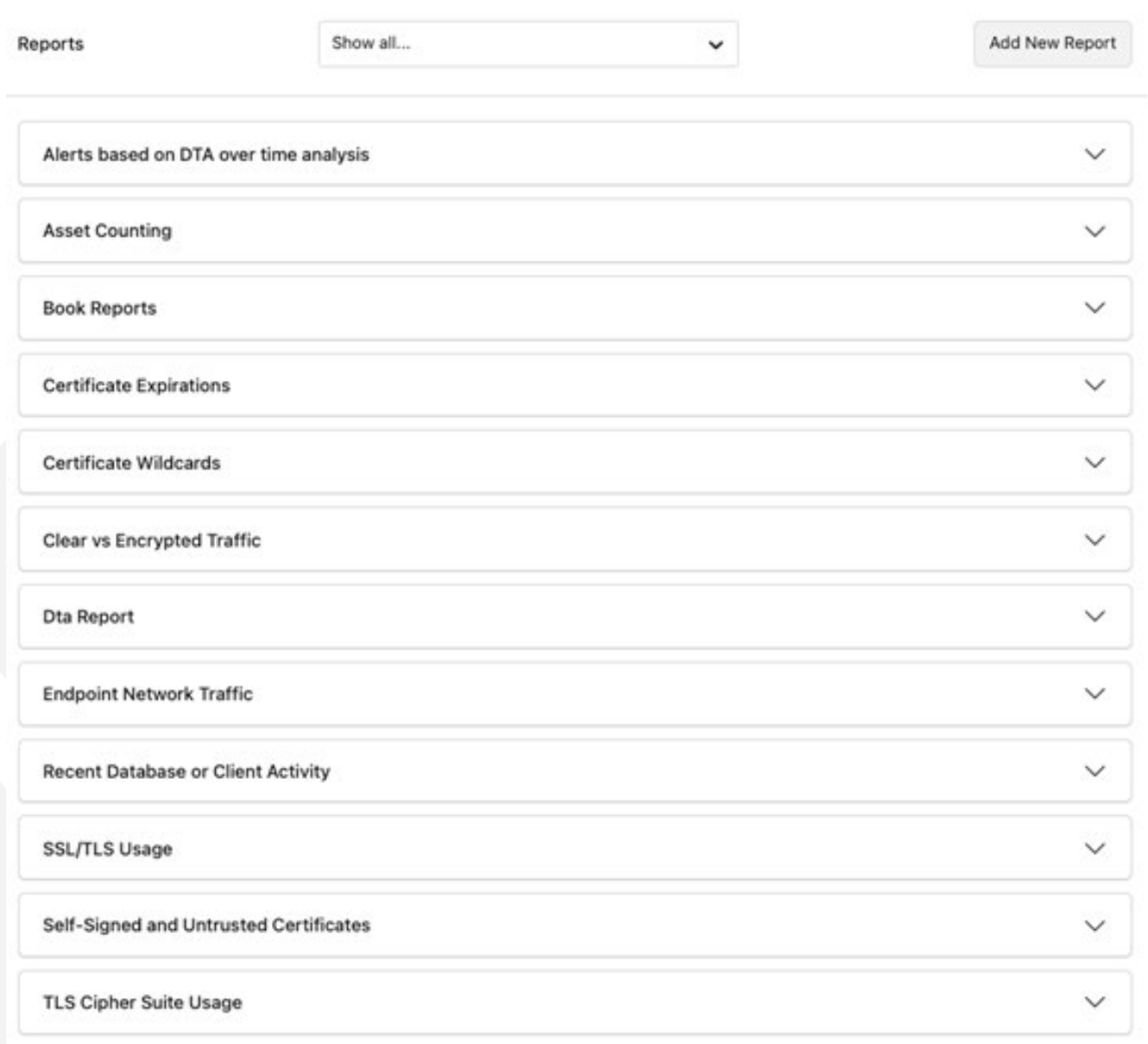
The server display shows a list of all sessions, including the client IP, certificates, and certificate chains in use for each session. Clicking a session will take you to the session detail page which includes encryption, traffic volume, and traffic rate information, along with details on the certificate chain.



6 Reports

The Reports page of the application provides access to pre-built reports on a variety of activity recorded by the system, along with any reports you have built using the Dta discovery page.

All reports run on the system then downloaded to a local machine for viewing. The page includes a summary of the most recently run reports on the right side of the screen. Those reports that have run will remain in the system until manually deleted. All reports provide details on the top five of each category reported.




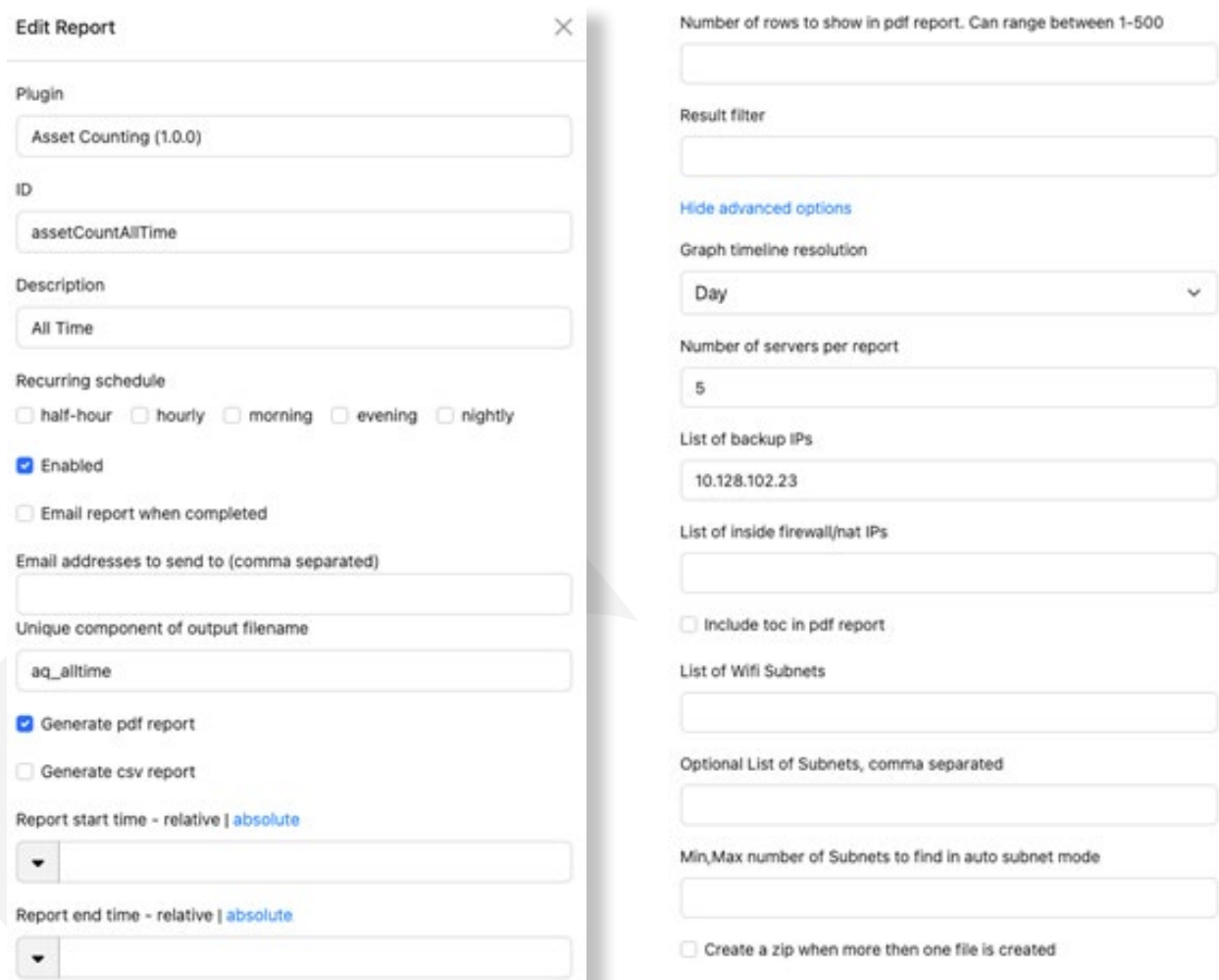
The screenshot shows the Reports page interface. At the top left is the word "Reports". To its right is a dropdown menu with the text "Show all..." and a downward arrow. Further right is a button labeled "Add New Report". Below these elements is a list of report categories, each in a white box with a downward arrow on the right side:

- Alerts based on DTA over time analysis
- Asset Counting
- Book Reports
- Certificate Expirations
- Certificate Wildcards
- Clear vs Encrypted Traffic
- Dta Report
- Endpoint Network Traffic
- Recent Database or Client Activity
- SSL/TLS Usage
- Self-Signed and Untrusted Certificates
- TLS Cipher Suite Usage

6.1 Asset Counting

The Asset Counting report provides a summary of IT assets by type as identified by the application software. This includes a breakdown of servers and server networks, clients, and users. The report can be configured to identify backups and wi-fi networks along with email security information. The report also provides subnet details on both clients and servers.

The report can be edited prior to running using the edit  button and run on a schedule:



Edit Report [Close]

Plugin
Asset Counting (1.0.0)

ID
assetCountAllTime

Description
All Time

Recurring schedule
 half-hour hourly morning evening nightly
 Enabled
 Email report when completed

Email addresses to send to (comma separated)
[Text Field]

Unique component of output filename
aq_alltime

Generate pdf report
 Generate csv report

Report start time - relative | [absolute](#)
[Dropdown]

Report end time - relative | [absolute](#)
[Dropdown]

Number of rows to show in pdf report. Can range between 1-500
[Text Field]

Result filter
[Text Field]

[Hide advanced options](#)

Graph timeline resolution
Day [Dropdown]

Number of servers per report
5

List of backup IPs
10.128.102.23

List of inside firewall/nat IPs
[Text Field]

Include toc in pdf report

List of Wifi Subnets
[Text Field]

Optional List of Subnets, comma separated
[Text Field]

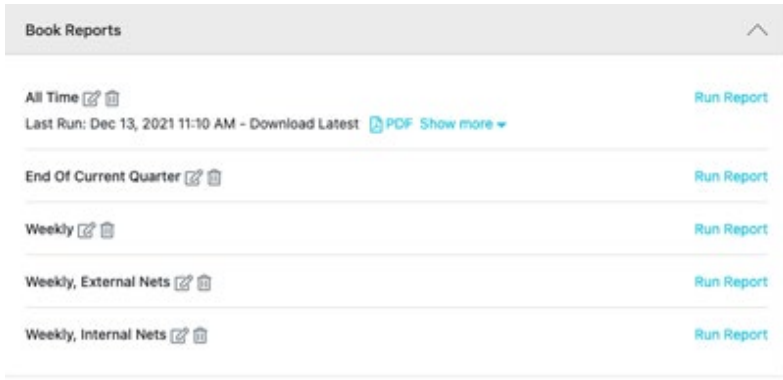
Min,Max number of Subnets to find in auto subnet mode
[Text Field]


Create a zip when more then one file is created

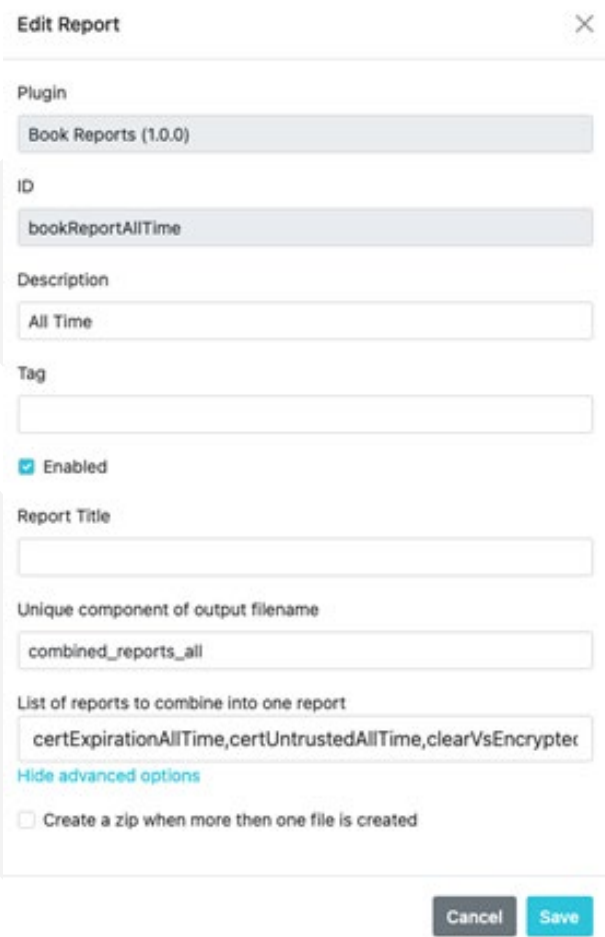
6.2 Book Reports

Book Reports are a compilation of all the pre-built reports the system generates. It includes sections including Certificate Expirations, Self-Signed and Untrusted Certificates, Clear vs Encrypted Traffic, Certificate Wildcards, SSL/TLS Usage, and TLS Cipher Suite Usage.

The reports can be run against traffic for All Time, End of Current Quarter, Weekly, Weekly on External network connections, and Weekly on Internal network connections.



Each report can be edited prior to running using the edit  button:



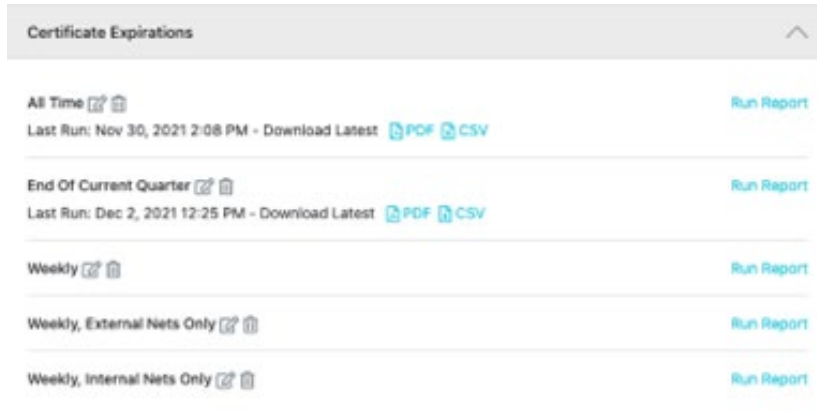
The 'Edit Report' dialog box contains the following fields and options:

- Plugin:** Book Reports (1.0.0)
- ID:** bookReportAllTime
- Description:** All Time
- Tag:** (empty field)
- Enabled
- Report Title:** (empty field)
- Unique component of output filename:** combined_reports_all
- List of reports to combine into one report:** certExpirationAllTime,certUntrustedAllTime,clearVsEncrypter
- [Hide advanced options](#)
- Create a zip when more then one file is created


Buttons: Cancel, Save

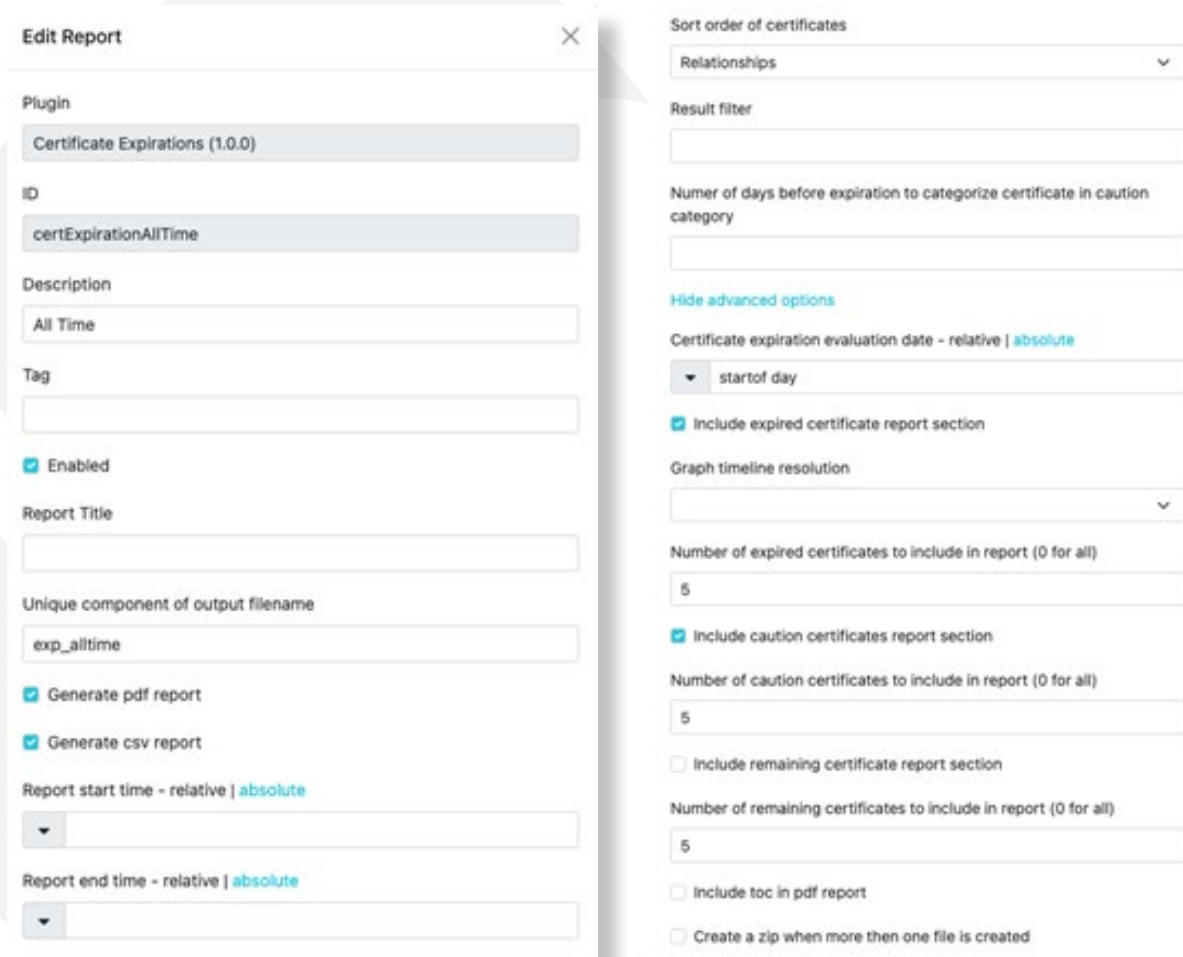
6.3 Certificate Expirations

The Certificate Expirations report shows you a summary of all certificate usage, certificates used after the expiration date, and weekly projected expirations.



The reports can be run against traffic for All Time, End of Current Quarter, Weekly, Weekly on External network connections, and Weekly on Internal network connections.

The report can be edited using the edit button  and has several options:




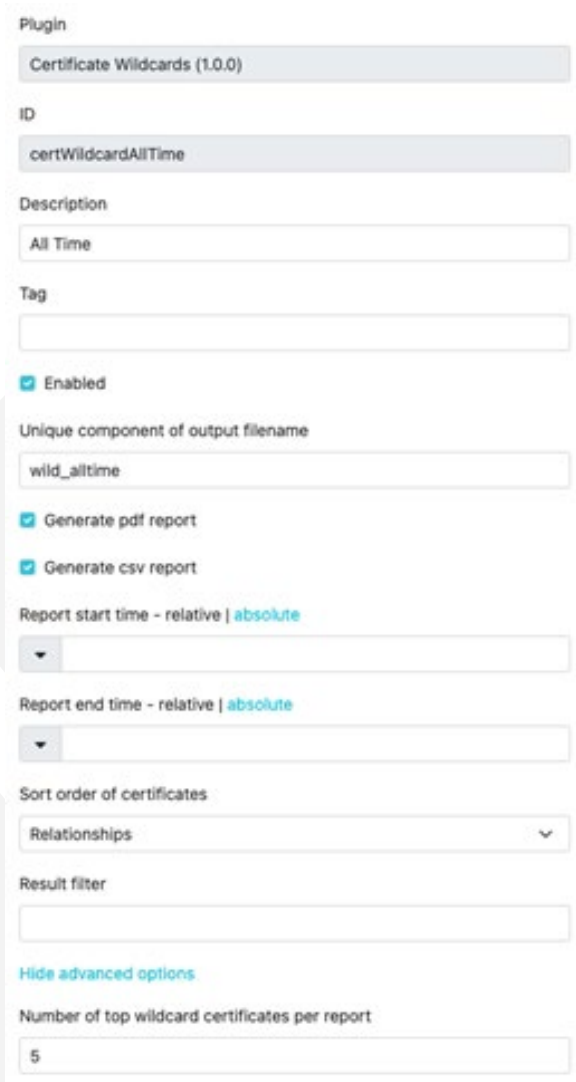
The report can be downloaded as a PDF or CSV. The CSV contains the details from the top five of each category in the report.

6.4 Certificate Wildcards

The Certificate Wildcards report provides details on wildcard certificates in use in the network. It provides information on levels of potential threat for wildcards:

- Good – no wildcard certificates
- Caution – simple wildcards
- Warning – malformed wildcards
- Danger – prefixed wildcards
- Violation – tld wildcard such as *.com

The report can be edited using the edit button  and has several options:



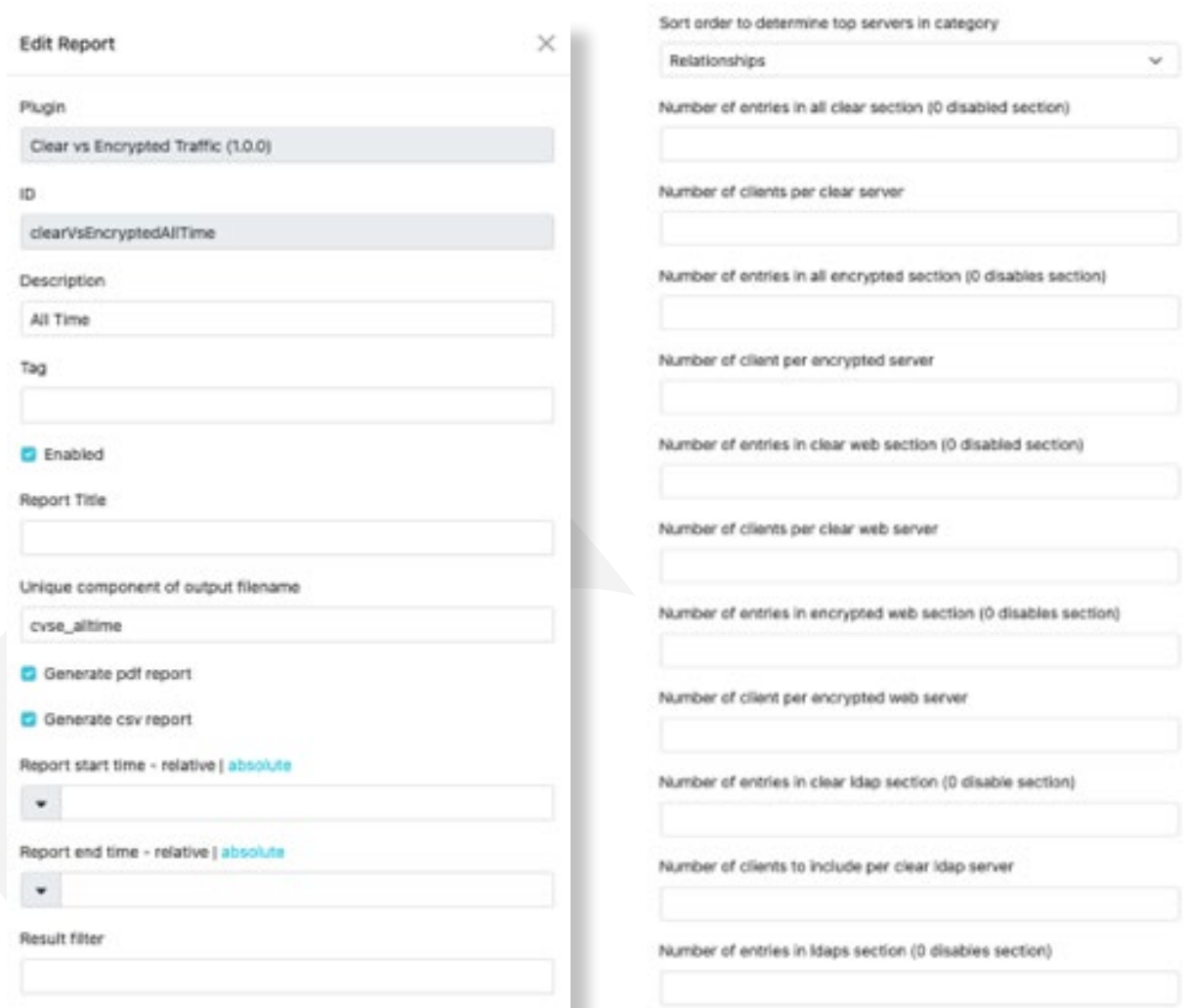
The screenshot shows a configuration form for the Certificate Wildcards report. The form includes the following fields and options:

- Plugin:** Certificate Wildcards (1.0.0)
- ID:** certWildcardAllTime
- Description:** All Time
- Tag:** (empty text field)
- Enabled**
- Unique component of output filename:** wild_alltime
- Generate pdf report**
- Generate csv report**
- Report start time - relative | absolute:** (dropdown menu)
- Report end time - relative | absolute:** (dropdown menu)
- Sort order of certificates:** Relationships (dropdown menu)
- Result filter:** (empty text field)
- [Hide advanced options](#)
- Number of top wildcard certificates per report:** 5

6.5 Clear vs Encrypted Traffic

The Clear vs Encrypted Traffic report provides summary and detailed analysis of all traffic captured by the system. The report includes information about all traffic, web traffic, LDAP traffic, database traffic, interactive traffic, and all other forms of traffic that cannot be classified in any of those categories. It includes trends and graphs of encrypted traffic by type. The report includes details on top five servers and clients running both encrypted and unencrypted traffic in each category.

The report can be edited using the edit button  and has several options:



Edit Report [X]

Plugin
Clear vs Encrypted Traffic (1.0.0)

ID
clearVsEncryptedAllTime

Description
All Time

Tag
[]

Enabled

Report Title
[]

Unique component of output filename
cvse_alltime

Generate pdf report

Generate csv report

Report start time - relative | absolute
[]

Report end time - relative | absolute
[]

Result filter
[]

Sort order to determine top servers in category
Relationships [v]

Number of entries in all clear section (0 disabled section)
[]

Number of clients per clear server
[]

Number of entries in all encrypted section (0 disables section)
[]

Number of client per encrypted server
[]

Number of entries in clear web section (0 disabled section)
[]

Number of clients per clear web server
[]

Number of entries in encrypted web section (0 disables section)
[]

Number of client per encrypted web server
[]

Number of entries in clear ldap section (0 disable section)
[]

Number of clients to include per clear ldap server
[]

Number of entries in ldaps section (0 disables section)
[]

Number of clients to include per ldap server

Number of entries in clear database section (0 disables section)

Number of client to include per clear database server

Number of entries in encrypted database section (0 disables section)

Number of clients to include per encrypted database server

Number of entries in clear interactive section (0 disables section)

Number of clients to include per clear interactive server

Number of entries in encrypted interactive section (0 disables section)

Number of clients to include per encrypted interactive server

Number of entries in other clear section (0 disables section)

Number of clients to include per clear other server


6.6 Dta Report

The Dta Report will display any reports that have been created by a user on the system using the Discover page.

Dta Report 

TLS Below 1.2   Run Report

Last Run: Dec 13, 2021 11:13 AM - Download Latest  

Each report can be edited using the edit button  and has the same options as those used to create the report originally.

6.7 Endpoint Network Traffic

The Endpoint Network Traffic report can be used to get detailed connection information about a specific server. Before running the report, you must use the edit button to open the report data and enter the Server IP you wish to report on.

Edit Report ✕

Plugin
Endpoint Network Traffic (1.0.0)

ID
endPointWeekly

Description
Weekly

Run nightly

Enabled

Report Title

Unique component of output filename
cvse_weekly

Generate pdf report

Generate csv report

Report start time - relative | [absolute](#)
startof day minus 7 days

Report end time - relative | [absolute](#)
startof day

Result filter

Server IP

[Show advanced options](#)

Advanced options for the report include:

<p>Sort order to determine top servers in category</p> <p>Relationships <input type="button" value="v"/></p>	<p>Number of clients to include per ldaps server</p> <input type="text"/>
<p>Number of entries in all clear section (0 disables section)</p> <input type="text"/>	<p>Number of entries in clear database section (0 disables section)</p> <input type="text"/>
<p>Number of clients per clear server</p> <input type="text"/>	<p>Number of client to include per clear database server</p> <input type="text"/>
<p>Number of entries in all encrypted section (0 disables section)</p> <input type="text"/>	<p>Number of entries in encrypted database section (0 disables section)</p> <input type="text"/>
<p>Number of client per encrypted server</p> <input type="text"/>	<p>Number of clients to include per encrypted database server</p> <input type="text"/>
<p>Number of entries in clear web section (0 disables section)</p> <input type="text"/>	<p>Number of entries in clear interactive section (0 disables section)</p> <input type="text"/>
<p>Number of clients per clear web server</p> <input type="text"/>	<p>Number of clients to include per clear interactive server</p> <input type="text"/>
<p>Number of entries in encrypted web section (0 disables section)</p> <input type="text"/>	<p>Number of entries in encrypted interactive section (0 disables section)</p> <input type="text"/>
<p>Number of client per encrypted web server</p> <input type="text"/>	<p>Number of clients to include per encrypted interactive server</p> <input type="text"/>
<p>Number of entries in clear ldap section (0 disable section)</p> <input type="text"/>	<p>Number of entries in other clear section (0 disables section)</p> <input type="text"/>
<p>Number of clients to include per clear ldap server</p> <input type="text"/>	<p>Number of clients to include per clear other server</p> <input type="text"/>
<p>Number of entries in ldaps section (0 disables section)</p> <input type="text"/>	<p>Number of entries in encrypted other section (0 disables section)</p> <input type="text"/>
	<p>Number of clients to include per encrypted other server</p> <input type="text"/>
	<p>Graph timeline resolution</p> <input type="text" value=""/>
	<p><input type="checkbox"/> Include toc in pdf report</p>
	<p><input type="checkbox"/> Create a zip when more than one file is created</p>
	<p><input type="button" value="Cancel"/> <input type="button" value="Save"/></p>

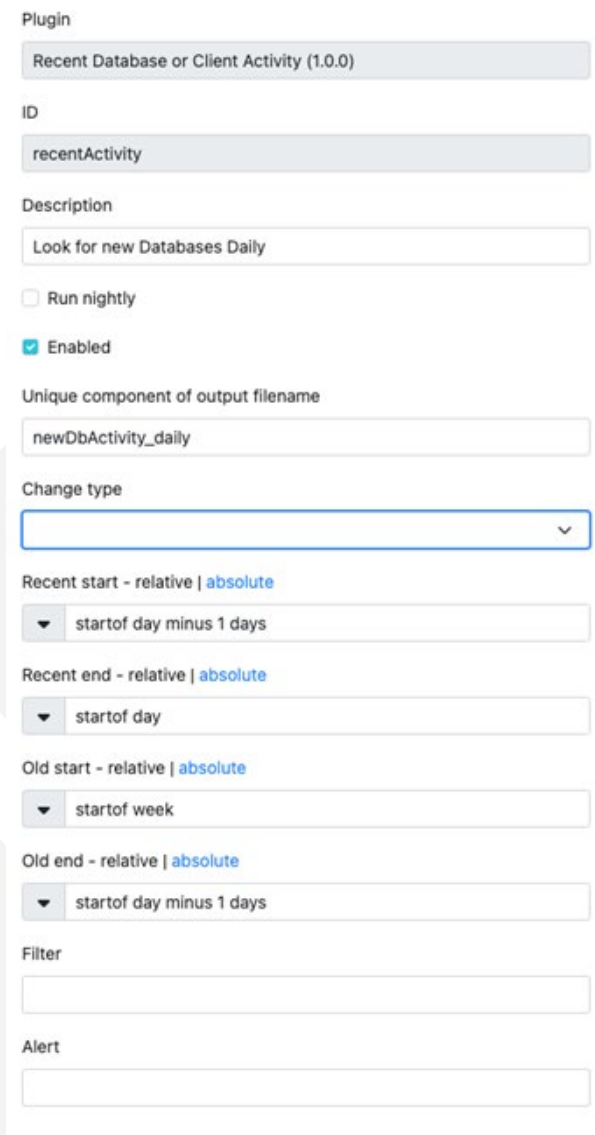
6.8 Recent Database or Client Activity

The Recent Database or Client Activity report can be used to send nightly alerts when new databases are discovered, or new clients are identified connecting to a database. Run the report nightly to send the alert. In addition, the email alert settings must be configured via the shell or command line and include an alert name that is entered into the report configuration.

Use Application Settings > Reports SMTP to configure the SMTP server that will process the report emails. See the CipherInsights Configuration and Management Guide for details.

The time window for comparison of previously seen vs new databases or client activity is configurable; the report is preconfigured to compare the previous day with the prior week leading up to that day.

To configure the report to run nightly, adjust the time range for viewing, set the alert for email or syslog notification, and determine if the report will include new databases or new clients connecting to an existing database, use the screens below.



The screenshot shows a configuration form for the 'Recent Database or Client Activity' plugin. The form includes the following fields and options:

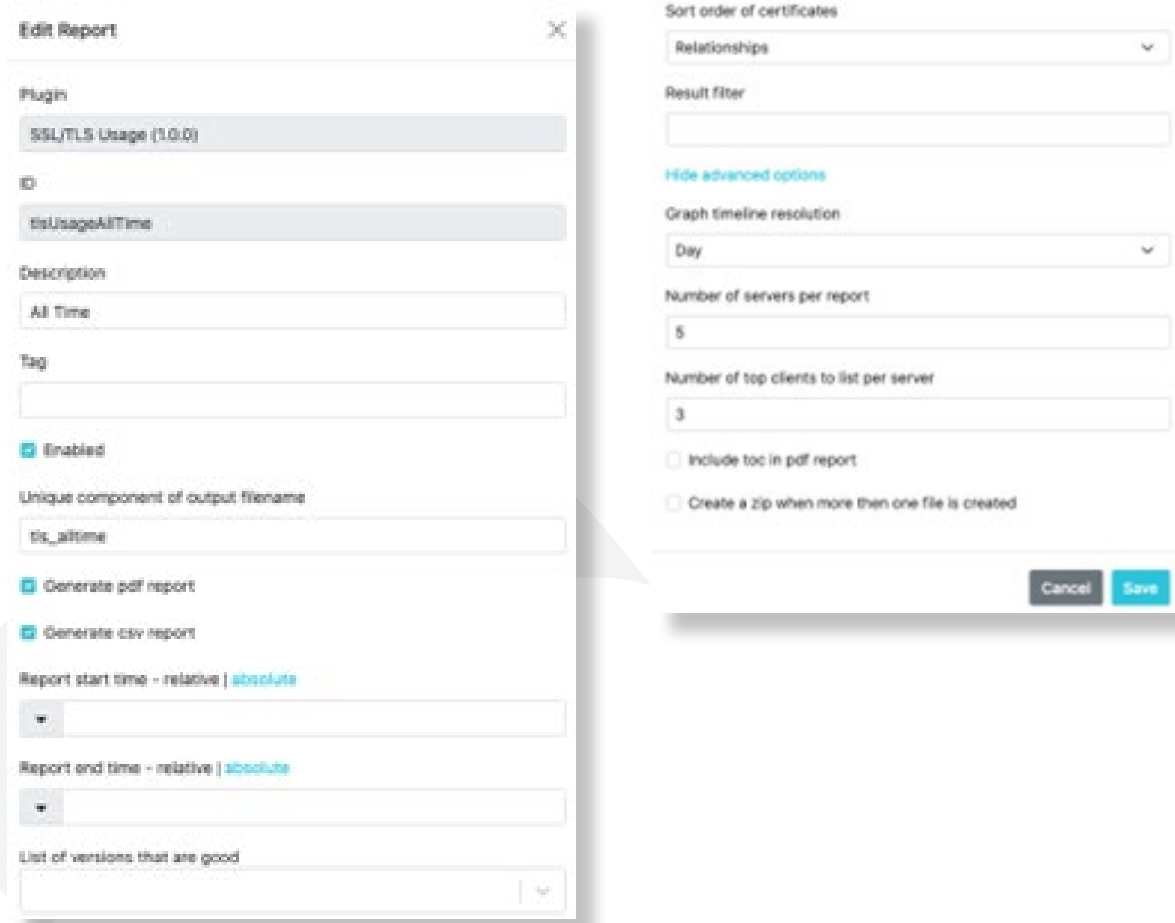
- Plugin:** Recent Database or Client Activity (1.0.0)
- ID:** recentActivity
- Description:** Look for new Databases Daily
- Run nightly
- Enabled
- Unique component of output filename:** newDbActivity_daily
- Change type:** (Dropdown menu)
- Recent start - relative | [absolute](#):** startof day minus 1 days
- Recent end - relative | [absolute](#):** startof day
- Old start - relative | [absolute](#):** startof week
- Old end - relative | [absolute](#):** startof day minus 1 days
- Filter:** (Text input field)
- Alert:** (Text input field)

6.9 SSL/TLS Usage

The SSL/TLS Usage report provides summary and detailed analysis of all traffic captured by the system with respect to encryption methods detected. It includes trends and graphs of encrypted traffic by type.

The report includes details on top 5 servers and clients running encryption levels below NIST recommended levels (SSL/V3, TLS1.0, and TLS1.1).

The report can be edited using the edit button  and has several options:



Edit Report [X]

Plugin
SSL/TLS Usage (1.0.0)

ID
tsUsageAllTime

Description
All Time

Tag
[]

Enabled

Unique component of output filename
ts_alltime

Generate pdf report

Generate csv report

Report start time - relative | absolute
[]

Report end time - relative | absolute
[]

List of versions that are good
[]

Sort order of certificates
Relationships

Result filter
[]

[Hide advanced options](#)

Graph timeline resolution
Day

Number of servers per report
5

Number of top clients to list per server
3

Include toc in pdf report

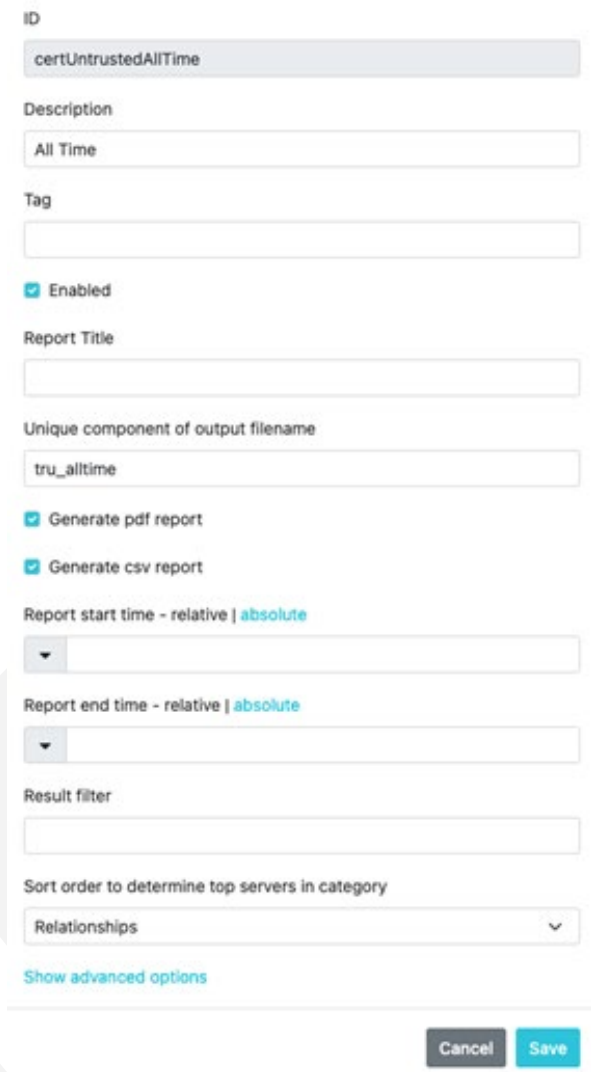
Create a zip when more than one file is created

Cancel Save

6.10 Self-Signed and Untrusted Certificates

The Self-Signed and Untrusted Certificates report provides summary and detailed information on untrusted or self-signed certificates. It includes an overview and a trend graph as well as a top five report that includes a list of servers using self-signed certificates.

The report can be edited using the edit button  and has several options:



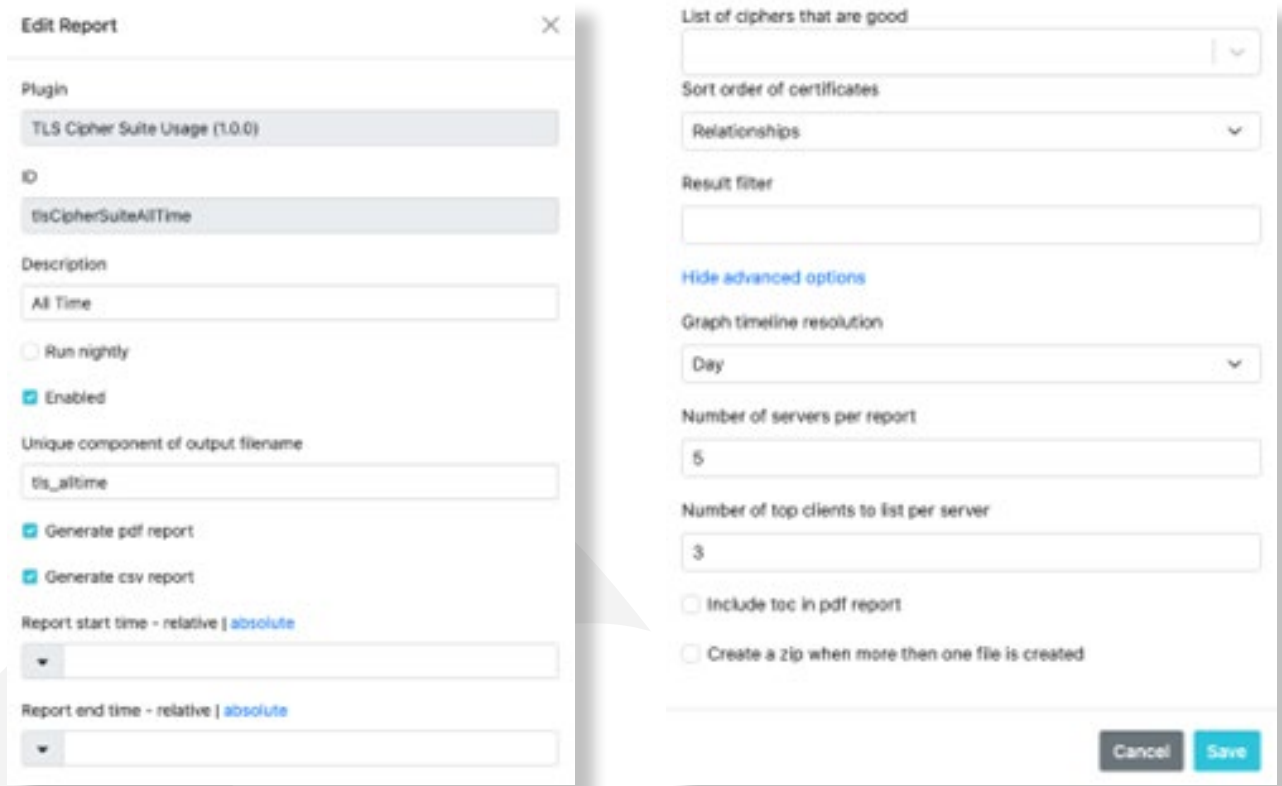
The screenshot shows a configuration form for a report. The fields and options are as follows:

- ID:** certUntrustedAllTime
- Description:** All Time
- Tag:** (empty field)
- Enabled**
- Report Title:** (empty field)
- Unique component of output filename:** tru_alltime
- Generate pdf report**
- Generate csv report**
- Report start time - relative | absolute:** (dropdown menu)
- Report end time - relative | absolute:** (dropdown menu)
- Result filter:** (empty field)
- Sort order to determine top servers in category:** Relationships
- [Show advanced options](#)
- Buttons:** Cancel, Save

6.11 TLS Cipher Suite Usage

The TLS Cipher Suite report provides summary information on TLS Ciphers used, Key Exchange Algorithms, Authentication Algorithms, Block Stream Ciphers, and Signature Algorithms. It also includes daily trending information and top five servers using obsolete ciphers.

The report can be edited using the edit button  and has several options:



Edit Report [Close]

Plugin
TLS Cipher Suite Usage (1.0.0)

ID
tlsCipherSuiteAllTime

Description
All Time

Run nightly
 Enabled

Unique component of output filename
tls_alltime

Generate pdf report
 Generate csv report

Report start time - relative | absolute
▼

Report end time - relative | absolute
▼

List of ciphers that are good
▼

Sort order of certificates
Relationships ▼

Result filter
▼

[Hide advanced options](#)

Graph timeline resolution
Day ▼

Number of servers per report
5

Number of top clients to list per server
3

Include toc in pdf report
 Create a zip when more than one file is created

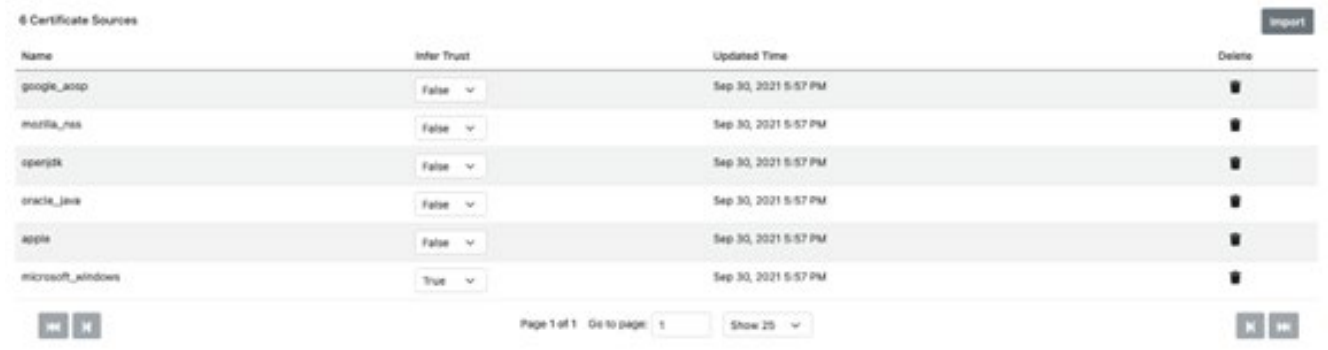
Cancel Save

7 Certificate Validation

The Application Settings > Certificate Sources page lists the validation settings and pre-programmed certificate sources (trust stores) and that can be used by the system to validate certificates.

7.1 Certificate Sources

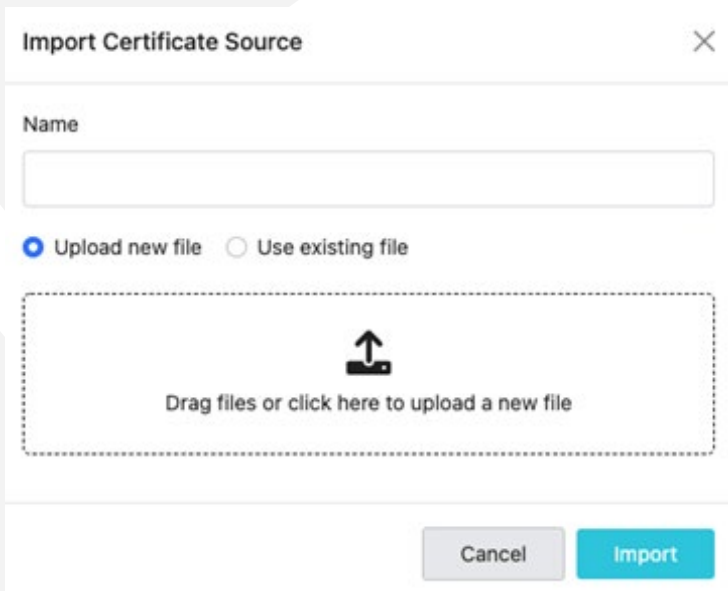
The Microsoft Windows trust store is the default store used by the application.



Name	Infer Trust	Updated Time	Delete
google_aosp	False	Sep 30, 2021 5:57 PM	
mozilla_nss	False	Sep 30, 2021 5:57 PM	
openssh	False	Sep 30, 2021 5:57 PM	
oracle_java	False	Sep 30, 2021 5:57 PM	
apple	False	Sep 30, 2021 5:57 PM	
microsoft_windows	True	Sep 30, 2021 5:57 PM	

You can choose to Import additional certificates that you want to include as trusted or build your own trust store. Create a file with the PEM of each certificate that you wish to be added to the system. Upload that file to the system using System > File Management.

Once the file is on the system, you may then use the Import button to add the new trust store to the system.



The file must be tarred and zipped so that it has a file extension of .gz for the system to recognize it. The file name structure must be xxx.pem.tar.gz.

7.2 Validation Settings

The Validation Settings page provides all the options that can be used by the system to validate certificates.

Validation Settings

- Check revocation using OCSP
- Ignore unhandled critical extensions
- Disable workarounds for broken certificates
- Enable proxy certificate validation
- Extended CRL features such as indirect CRLs, alternate CRL signing keys
- Delta CRL support
- Check self-signed CA signature
- Use trusted store first
- Allow partial chains if at least one certificate is in trusted store
- Do not try alternate chains
- Automatic validation of certificates

Maximum number of validations running at once

The options for validation, with explanation and defaults, are listed in the table below.

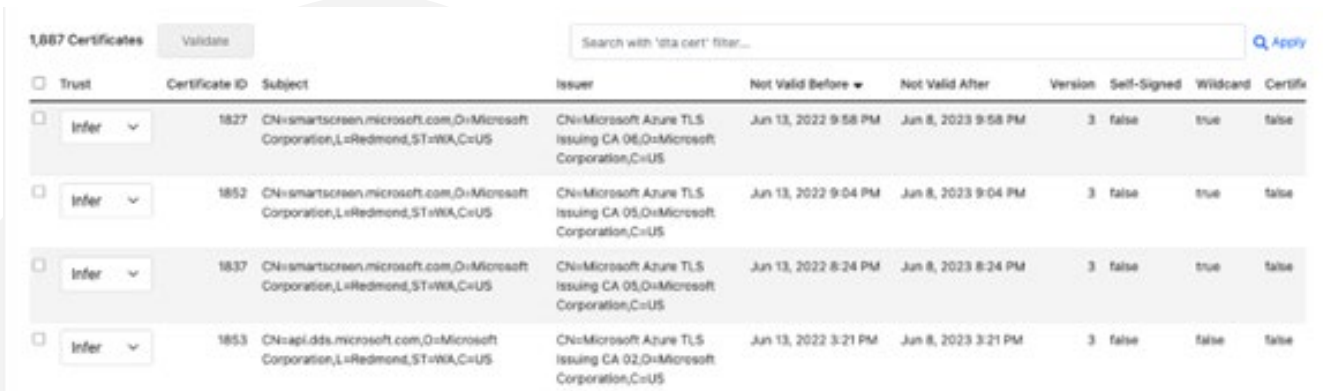
Table 7-1. Validation Fields

Field	Description	Options/Format
Check revocation using OCSP	Determine if the system will OSCP to check revocation of certificates	No
Ignore unhandled critical extensions	Tells the system what to do if an unhandled critical extension error is experienced while reading the cert	Yes
Disable workarounds for broken certificates	Determines if the system will allow workarounds for bad certificates	No
Enable proxy certificate validation	If a proxy certificate is identified, determine if the system will validate that cert	Yes
Extended CRL features such as indirect CRLs, alternate CRL signing keys	Determine processing of certificate revocation lists	Yes

Field	Description	Options/Format
Delta CRL support	Tells the system whether to use the Delta CRLs to determine if a certificate has been revoked	Yes
Check self-signed CA signature	Determines if the system will evaluate signatures of self-signed certificates	Yes
Use trusted store first	Determines if the system will use the trust store initially to validate certificates	Yes
Allow partial chains if at least one certificate is in trusted store	Tells the system whether to allow partial chains for validation	Yes
Do not try alternate chains	Tells the system whether to use alternate chains for validation	No
Maximum number of validations running at once	Number of certification validation processes that can run at any one time. Leave this number at the default.	1
Automatic validation of certificates	Tells the system whether to validate certificates	Yes

7.3 Updating Individual Certificate Settings

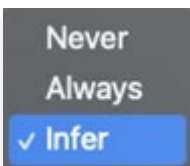
At the bottom of the certificate validation page is the list of each certificate the software has detected while monitoring.



Trust	Certificate ID	Subject	Issuer	Not Valid Before	Not Valid After	Version	Self-Signed	Wildcard	Certify
<input type="checkbox"/> Infer	1827	CN=smartscreen.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US	CN=Microsoft Azure TLS Issuing CA 06,O=Microsoft Corporation,C=US	Jun 13, 2022 9:58 PM	Jun 8, 2023 9:58 PM	3	false	true	false
<input type="checkbox"/> Infer	1852	CN=smartscreen.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US	CN=Microsoft Azure TLS Issuing CA 05,O=Microsoft Corporation,C=US	Jun 13, 2022 9:04 PM	Jun 8, 2023 9:04 PM	3	false	true	false
<input type="checkbox"/> Infer	1837	CN=smartscreen.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US	CN=Microsoft Azure TLS Issuing CA 05,O=Microsoft Corporation,C=US	Jun 13, 2022 8:24 PM	Jun 8, 2023 8:24 PM	3	false	true	false
<input type="checkbox"/> Infer	1853	CN=api.dds.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US	CN=Microsoft Azure TLS Issuing CA 02,O=Microsoft Corporation,C=US	Jun 13, 2022 3:21 PM	Jun 8, 2023 3:21 PM	3	false	false	false

The default validation setting for each certificate is "Infer," which means it will use the system certificate sources to determine if a certificate is valid. That configuration can be adjusted on a per-certificate basis using this screen.

Select the Trust option drop down and select the option you wish to set.

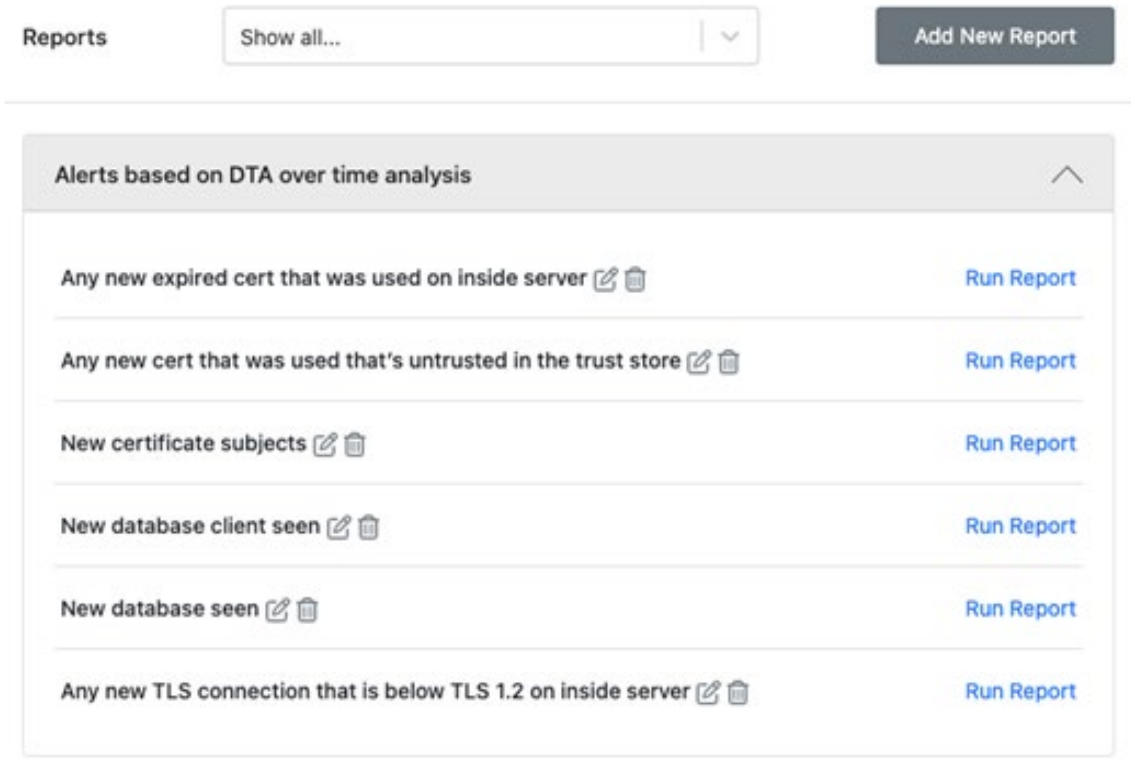


8 System Alerts

The application can send alerts on a scheduled basis for a pre-determined set of activity identified by the software. These alerts are found on the Reports page.

The activities include:

- Any new expired certificate used on an internal server
- Any new certificate used that was not in the configured trust store
- Any new certificate subjects identified
- New database clients detected
- New database services detected
- Any new TLS connection below TLS1.2 on an internal server



The screenshot shows the 'Reports' section of the application. At the top, there is a 'Reports' label, a dropdown menu set to 'Show all...', and an 'Add New Report' button. Below this is a section titled 'Alerts based on DTA over time analysis' with an expand/collapse arrow. The list contains six items, each with a configuration icon (pencil) and a delete icon (trash), and a 'Run Report' button on the right:

- Any new expired cert that was used on inside server
- Any new cert that was used that's untrusted in the trust store
- New certificate subjects
- New database client seen
- New database seen
- Any new TLS connection that is below TLS 1.2 on inside server

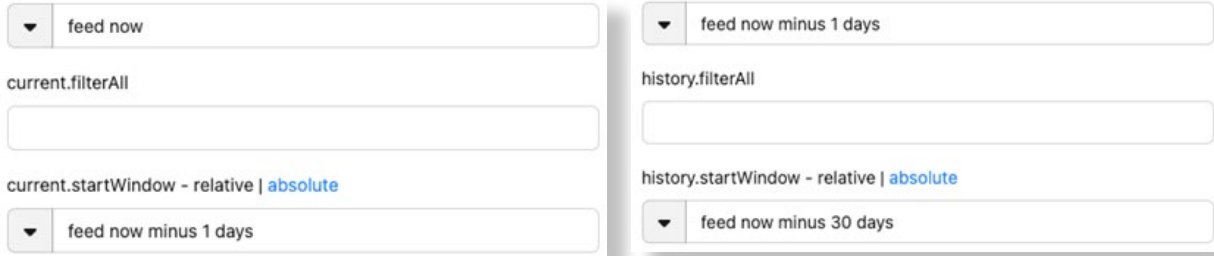
These reports/alerts can be run manually with the Run Report button, or automatically by configuring the alert to run on a scheduled basis using the configuration button. Options for alert timing include half-hour, hourly, morning, evening, or nightly.

Recurring schedule

- half-hour hourly morning evening nightly

The alerts are configured with windows of time relative to the current feed time. The application compares the current window with the history window to determine if any new item has been identified, and alerts if it finds something new.

The default configuration is for a daily alert, so the windows are:



The screenshot shows two side-by-side configuration panels. The left panel has a dropdown menu set to 'feed now', a text input field for 'current.filterAll', and a radio button selection for 'current.startWindow - relative | absolute' with 'absolute' selected. Below this is another dropdown menu set to 'feed now minus 1 days'. The right panel has a dropdown menu set to 'feed now minus 1 days', a text input field for 'history.filterAll', and a radio button selection for 'history.startWindow - relative | absolute' with 'absolute' selected. Below this is another dropdown menu set to 'feed now minus 30 days'.

In the example shown, the system looks at data starting one day prior (feed now minus 1 day) up to the current time (feed now), then compares that to 30 days (feed now minus 30 days) prior up to one day prior (feed now minus 1 days).

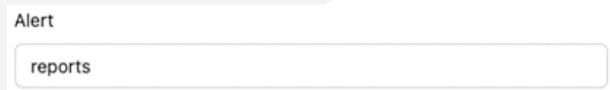
Those windows will be adjusted if the alerts are scheduled on a more frequent (half-hour, hourly) basis.

The Alert option determines how the alert will be delivered. The application creates a set of default alerts that sends the message via syslog. For example, the expired certificate alert uses:



The screenshot shows a dropdown menu labeled 'Alert' with the option 'sysloggerExpiredCert' selected.

The system can be configured to send the alerts via email by changing the alert to "reports" and configuring the Application Settings > Reports SMTP page.



The screenshot shows a dropdown menu labeled 'Alert' with the option 'reports' selected.

QUANTUMXCHANGE™

Certificate of Compliance

**Awarded To
Demo**

This is to certify that Demo has no cleartext passwords

**Compliance Covered
Password Exposure**

**Evaluation Period: 30 days
Network Nodes Monitored: 8630
Risk Discovery License Expiration: Never**

Holly A Neiveem

**Holly A Neiveem
Quantum Xchange, CFO**

**Certificate ID:
65cf65e5bfaea8413738bead459b0945**

Issued On: 2023-07-13T20:37:52.184Z

Conditions of issuing:

1. Quantum Xchange has issued this certificate to indicate that the company's user authentication environment has been validated against industry cryptographic standard for strong as of the Date of Compliance stated below.
2. This certificate is valid through the expiration of the risk assessment license.
3. The assessment shall not warrant or guarantee to any third party that the company's environment is invulnerable to attack or compromise.
4. This certificate is issued by Quantum Xchange as a commercial representation of work completed.

Filter: No Filter