

Reports in LevelBlue TDR for Gov



LevelBlue Threat Detection and Response for Government (LevelBlue TDR for Gov) generates the following reports:

- **My Reports:** These are reports that you generate when viewing assets, asset groups, alarms, events, vulnerabilities, or configuration issues in LevelBlue TDR for Gov. You can choose the format of the reports between HTML and CSV. See [My Reports](#) for more information.
- **Compliance Reports:** These are reports built on templates defined for various compliance standards, including Payment Card Industry (PCI), National Institute of Standards Technology Cybersecurity Framework (NIST CSF), Health Insurance Portability and Accountability Act (HIPAA), and ISO 27001. The reports are based on alarms, vulnerabilities, or events collected in the system. See [Compliance Templates](#) for more information.
- **Event Type Reports:** These are reports built on templates specific for events, by data sources or type of data source. See [Event Type Templates](#) for more information.

My Reports

In LevelBlue TDR for Gov, you can generate reports when viewing assets, asset groups, alarms, events, vulnerabilities, and configuration issues. If you save these reports, you can later run them again through the primary menu (Reports > My Reports). The history of your reports are grouped into report category and report format for easy access.

You can filter your reports using the options in the Search and Filters area on the left side of the page. There are six report categories (assets, asset groups, alarms, events, vulnerabilities, and configuration issues) and two report formats (HTML and CSV).

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the  icon to hide the filter pane. Click the  icon to expand the filter pane. The table below explain what each column means.

List of Columns on the Export History Page

Column Field Name	Description
Report Title	Title given to the report
Format	Format on which the report was last run
Limit	Number of records that the report contains
Category	Report category
Created by	Email address of the person who created the report
Run Date	Date on which the report was run

You can choose the number of items to display by selecting **20**, **50**, or **100** below the table.


To generate a report

1. Navigate to **Activity > Alarms**.

The procedure is the same for events, assets, asset groups, vulnerabilities, and configuration issues. The Generate Report link is available on their respective pages.

2. Select the items you want to include in the report.
3. Click **Generate Report**.

The Configure Report window displays.

4. Enter or modify the name of the report.
5. (Optional.) Enter or modify the description of the report.
6. Select a date range.
 - a. If your report contains alarms or events, you can select a predefined range of **last hour**, **last 24 hours**, **last 7 days**, **last 30 days**, or **last 90 days**. You can also set your own date range by clicking the calendar icon .
 - b. If your report contains vulnerabilities or configuration issues, you can use the calendar entry fields to set your own date range.
7. Select the export format: **CSV** or **HTML**.

If you choose HTML, a new tab opens in your browser, displaying the report. You can click **Print** to print the report or save it as PDF.

If you choose CSV, your browser downloads the report automatically.



Note: Adblock blocks the download of CSV reports. To avoid this, you need to add the URL of your LevelBlue TDR for Gov instance as an exception in Adblock.

8. Choose the number of records to export.
9. For HTML format, you will see a Graphs section. Use this section to include additional graphs in your report. There may be some graphs already selected, but you can add or remove graphs that you want to include by clicking the right arrow icon (➔) or left arrow icon (➠).
10. Click the **Save Report** checkbox if you want to generate the report again in the future. You can find the saved reports on Reports > My Reports.
11. Click **Generate Report**.

Your browser downloads the CSV report automatically or opens the HTML report in a different tab.

To run the same report again, go to Reports > My Reports and click the saved report. If you want, you can change any of the configuration before generating the report.

Compliance Templates

LevelBlue Threat Detection and Response for Government provides pre-built compliance templates to generate reports based on alarms, vulnerabilities, and events collected in the system. These reports make it fast and simple to navigate the requirements and demonstrate compliance during an audit. You can easily customize, save, and export any report as needed.

You can find these templates on **Reports > Compliance Templates**.

LevelBlue TDR for Gov supports the following compliance templates :

- **PCI:** The Payment Card Industry Data Security Standards (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. These reports are identified and based on specific PCI DSS requirements to provide the auditor with the specific information requested.



Note: The PCI compliance templates are based on the predefined PCI DSS Asset Group by default; however, you can select another asset group by customizing the template as described below.

- **NIST CSF:** The National Institute of Standards Technology Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.
- **HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. This includes covered entities, anyone who provides treatment, payment and operations in healthcare, and business associates, anyone with access to patient information and provides support in treatment, payment, or operations. Subcontractors, or business associates of business associates, must also be in compliance.



Note: The HIPAA compliance templates are based on the predefined HIPAA Asset Group by default; however, you can select another Asset Group by customizing the template as described below.

- **ISO 27001.** ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The ISO and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an information security management system (ISMS).

Each template listing includes these links:

- **View:** Opens a specific page of your environment.
- **Generate Report:** Opens the Configure Report window. You can define a name, a description, a date range, the output format, the number of records, and the additional view you want to include in your report.

To generate a report


1. Navigate to **Reports > Compliance Templates**.

The Compliance Templates page displays.

2. Select a template from the menu on the left.
3. Click the **Generate Report** link on the report you want to run.

The Configure Report window displays.

4. Enter or modify the name of the report.
5. (Optional.) Enter or modify the description of the report.
6. Select a date range.



- a. If your report contains alarms or events, you can select a predefined range of **last hour**, **last 24 hours**, **last 7 days**, **last 30 days**, or **last 90 days**. You can also set your own date range by clicking the calendar icon ().
 - b. If your report contains vulnerabilities or configuration issues, you can use the calendar entry fields to set your own date range.
7. Select the export format: **CSV** or **HTML**.

If you choose HTML, a new tab opens in your browser, displaying the report. You can click **Print** to print the report or save it as PDF.

If you choose CSV, your browser downloads the report automatically.



Note: Adblock blocks the download of CSV reports. To avoid this, you need to add the URL of your LevelBlue TDR for Gov instance as an exception in Adblock.

8. Choose the number of records to export.
9. For HTML format, you will see a Graphs section. Use this section to include additional graphs in your report. There may be some graphs already selected, but you can add or remove graphs that you want to include by clicking the right arrow icon () or left arrow icon ().
10. Click the **Save Report** checkbox if you want to generate the report again in the future. You can find the saved reports on Reports > My Reports.
11. Click **Generate Report**.

Your browser downloads the CSV report automatically or opens the HTML report in a different tab.

Event Type Templates

LevelBlue Threat Detection and Response for Government includes a set of predefined templates based on the classification of data sources or type of data source.

You can find these templates on **Reports > Event Type Templates**.

These are the predefined templates:

- **Type of Data Source:** Event Type Templates enable you to easily run a general firewall, authentication, and other types of normalized queries that do not require you to build complex filters based on specific plugin or event types. USM Anywhere supports the following

reports: Anomaly Detection, Antivirus, Application, Application Firewall, Authentication, Authentication and DHCP, Cloud Application, Cloud Infrastructure, DNS Server, Data Protection, Database, Endpoint Protection, Endpoint Security, Firewall, IDS, Infrastructure Monitoring, Intrusion Detection, Intrusion Prevention, Load Balancer, Mail Security, Mail Server, Management Platform, Network Access Control, Operating System, Other Devices, Proxy, Router, Router/Switch, Server, Switch, Unified Threat Management, VPN, Web Server, Wireless Security/Management.

- **Data Sources:** You can find templates based on the most commonly used data sources including but not limited to network-based intrusion detection system (NIDS), Amazon Web Services (AWS), Amazon DynamoDB, Amazon Simple Storage Services (S3), Amazon Virtual Private Cloud (VPC) Flow Logs, AWS Load Balancers, Microsoft Azure, Cisco Umbrella, Cylance, FireEye, FortiGate, Google G Suite, Microsoft Office 365, Okta, Palo Alto, SonicWALL, Sophos UTM, WatchGuard, VMware, Windows, LevelBlue Agent. There is also a template for the LevelBlue Generic Plugin.

Each report listing includes the Generate Report link, which opens the Configure Report window. You can define a name, a description, a date range, the output format, the number of records, and the additional view you want to include in your report.


To generate a report

1. Navigate to **Reports > Event Type Templates**.

The Event Type Templates page displays.

2. Select a template.
3. Click the **Generate Report** link on the report you want to run.

The Configure Report window displays.

4. Enter or modify the name of the report.
5. (Optional.) Enter or modify the description of the report.
6. Select a date range.
 - a. If your report contains alarms or events, you can select a predefined range of **last hour**, **last 24 hours**, **last 7 days**, **last 30 days**, or **last 90 days**. You can also set your own date range by clicking the calendar icon .
 - b. If your report contains vulnerabilities or configuration issues, you can use the calendar entry fields to set your own date range.
7. Select the export format: **CSV** or **HTML**.

If you choose HTML, a new tab opens in your browser, displaying the report. You can click **Print** to print the report or save it as PDF.

If you choose CSV, your browser downloads the report automatically.



Note: Adblock blocks the download of CSV reports. To avoid this, you need to add the URL of your LevelBlue TDR for Gov instance as an exception in Adblock.

8. Choose the number of records to export.
9. For HTML format, you will see a Graphs section. Use this section to include additional graphs in your report. There may be some graphs already selected, but you can add or remove graphs that you want to include by clicking the right arrow icon (➡) or left arrow icon (⬅).
10. Click the **Save Report** checkbox if you want to generate the report again in the future. You can find the saved reports on Reports > My Reports.
11. Click **Generate Report**.

Your browser downloads the CSV report automatically or opens the HTML report in a different tab.