Lightning Customer Portal
User Manual for Single Portal User

Version 1.3
6/2/2025

Revised On	Version	Description	Author
4/13/2022	1.0	Document Creation	CB, JM
12/23/2022	1.2	Updated to outSOC Release 2.8.0	Update Team
6/2/2025	1.3	Updated to Lightning Customer Portal rather than outSOC	CE

Contents

SilverSky is an award-winning, cybersecurity industry leader with more than 20 years of experience protecting businesses large and small. Customers count on the SilverSky team to deliver services that act as an extension of their security teams and to improve their security risk posture with SilverSky's flexible approach and skilled team members focused on the mission of safeguarding customer environments.

The Lightning Customer Portal, formerly known as outSOC, is a technology platform that optimizes the productivity and accuracy of the SilverSky Security Operations Center (SOC) and enables SOC analysts to identify and mitigate security threats on a customer's behalf. Available to both Managed Security Services customers and Lightning MDR platform customers, the Lightning Portal is a multi-tier, cloud-hosted, technology platform with multi-lingual, multi-time zone and hierarchical capabilities that provides automatically triggered response plans and incident notifications.

The objective of this guide is to provide an overview of the Lightning Portal application functionality and features. Please note, this guide does not provide recommendations about specific security settings, as those topics are beyond the scope of this document.

Screenshots are used throughout the manual to help orient content descriptions with visual elements of the portal. Content is redacted where necessary. Note that several images within the document contain the outSOC logo, which may look different in your Lightning portal experience.

Audience

This is a customer user manual for those who have a single Lightning Portal. This manual can be a helpful resource, but it is not intended for partners who manage multiple customers or for MSSP users.

Permissions for the Lightning Portal platform are set at the User level, therefore, not all Users will have the same access to features and functionality within the platform. This manual contains functionality descriptions for a typical single portal User account. Individual Users will be set up with Lightning Portal User permissions as part of the SilverSky service onboarding. Additional permissions can be requested using the support ticket feature.

SilverSky SOC Support Team

The SilverSky SOC support team is committed to customer success and is available to answer questions in a timely manner. Below is a table which outlines the best routes for requesting different types of support.

Support Needed	Best Route
Lightning Portal technical support	Create a ticket in the Lightning Portal
Lightning Portal security support	Create a ticket in the Lightning Portal
General SilverSky service inquiries Login support	Project Coordinator (during onboarding) Account Manager (after onboarding) supportdb@SilverSky.com
Emergency support	919.228.2559
Contact sales	Learn@silversky.com

Access and Login

The Lightning Portal can be accessed at https://platform.ousoc.com. It is recommended to bookmark this webpage in a preferred browser.

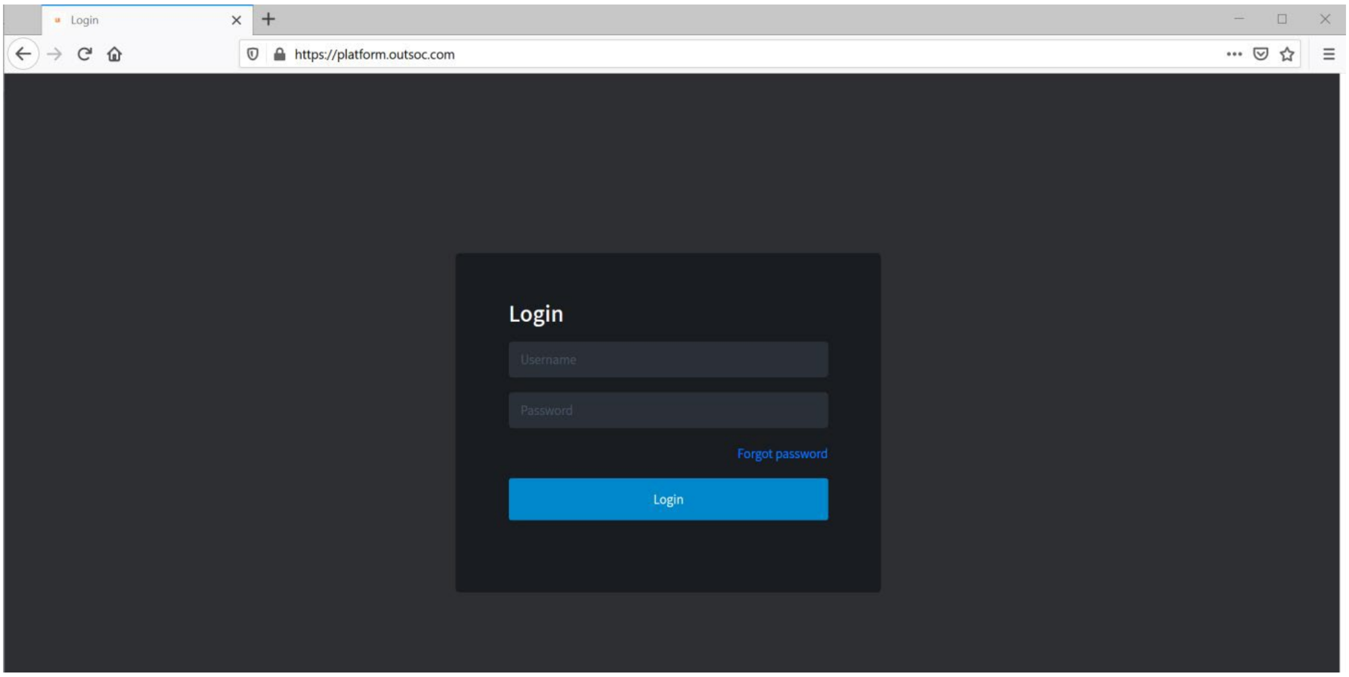


Figure 1: Lightning Portal Login Page

Login

Once a User account is created, the customer will receive personal login credentials from the SilverSky support team. If initial login credentials are not received, please contact the SilverSky deployment project coordinator (during onboarding) or account manager (after onboarding is complete). If additional user login credentials are required, please create a support ticket within the Lightning Portal.

Forgot Password

If a password is forgotten, select Forgot Password to initiate the self-service password reset process shown in Figure 2 below.

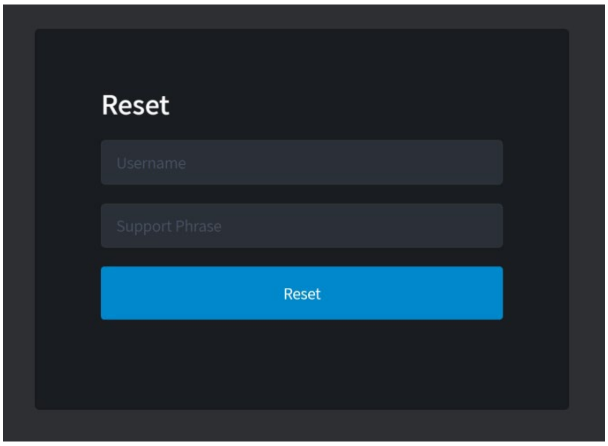
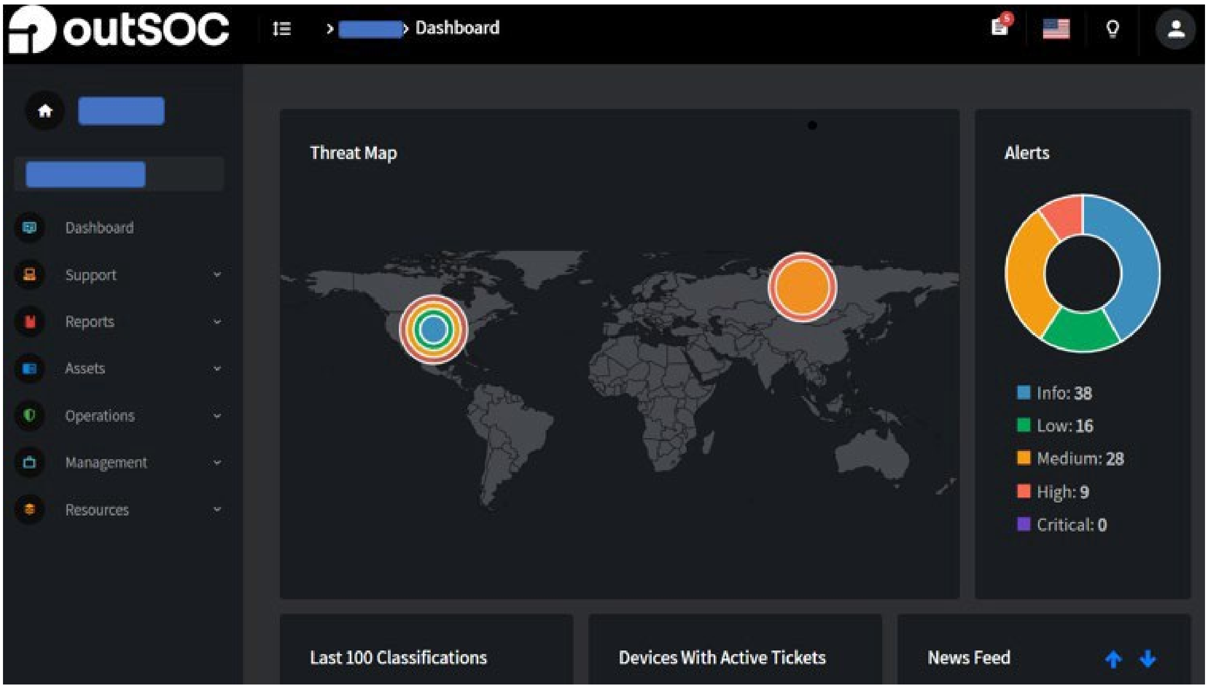


Figure 2: Forgot Password Reset

1. Enter username
2. Support phrase
    a. If the portal was set up with a support phrase:



        i. Enter the support phrase
        ii. Select Reset (Note: the Reset button will only work if the correct support phrase is entered.)
    b. If the portal was not set up with a support phrase, leave that box blank and select Reset.

A successful password reset request will look like Figure 3 shown below:

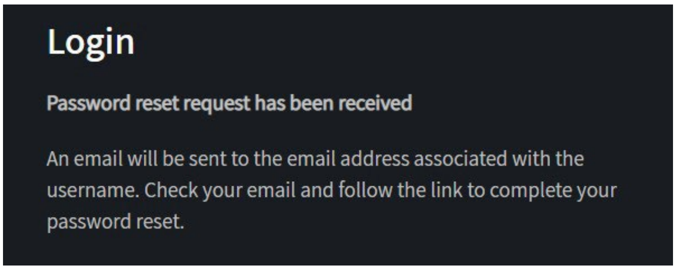


Figure 3: Password Reset Confirmation

Navigation

Upon login, access is granted to the Lightning Portal (see Figure 4 below). The portal navigation has three main sections:

1. Top Navigation Bar
2. Dashboard (populated with widgets)
3. Side Navigation Bar (hidden from view by default)

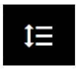
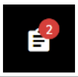
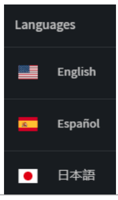
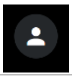
Note: Available menu options and widgets may appear different depending on subscribed services and User permissions.

Figure 4: Lightning Portal

Top Navigation Bar

The Top Navigation Bar is comprised of the following items (see Figure 5 below):

Figure 5: Top Navigation Bar

	**Menu Icon:** Select the menu icon to minimize or expand the Side Navigation Bar.
	**Portal Tag > Current View:** Displays the Portal Tag (a six character customer account code) and the current view.
	**Bulletins:** Select the bulletins icon to quickly access recent security bulletins posted. The number in red indicates the count of bulletins available for quick review.
	**Language:** The flag icon allows the adjustment of the language displayed on the Lightning Portal. Many of the reports and portal screens will be automatically translated to the selected language. If a language required is not displayed, please [create a support ticket] to make that request.
	**Portal Theme:** The light bulb icon allows users to toggle between dark and light themes.
	**View Profile/Log Out:** Allows a User to view User profile information and/or logout of the portal.

Dashboard

The Dashboard is a landing page that provides a quick summary of important security information via a collection of widgets. The default widgets included are the Threat Map, Alerts, Last 100 Classifications, Devices with Active Tickets, News Feed and Recent Incidents.

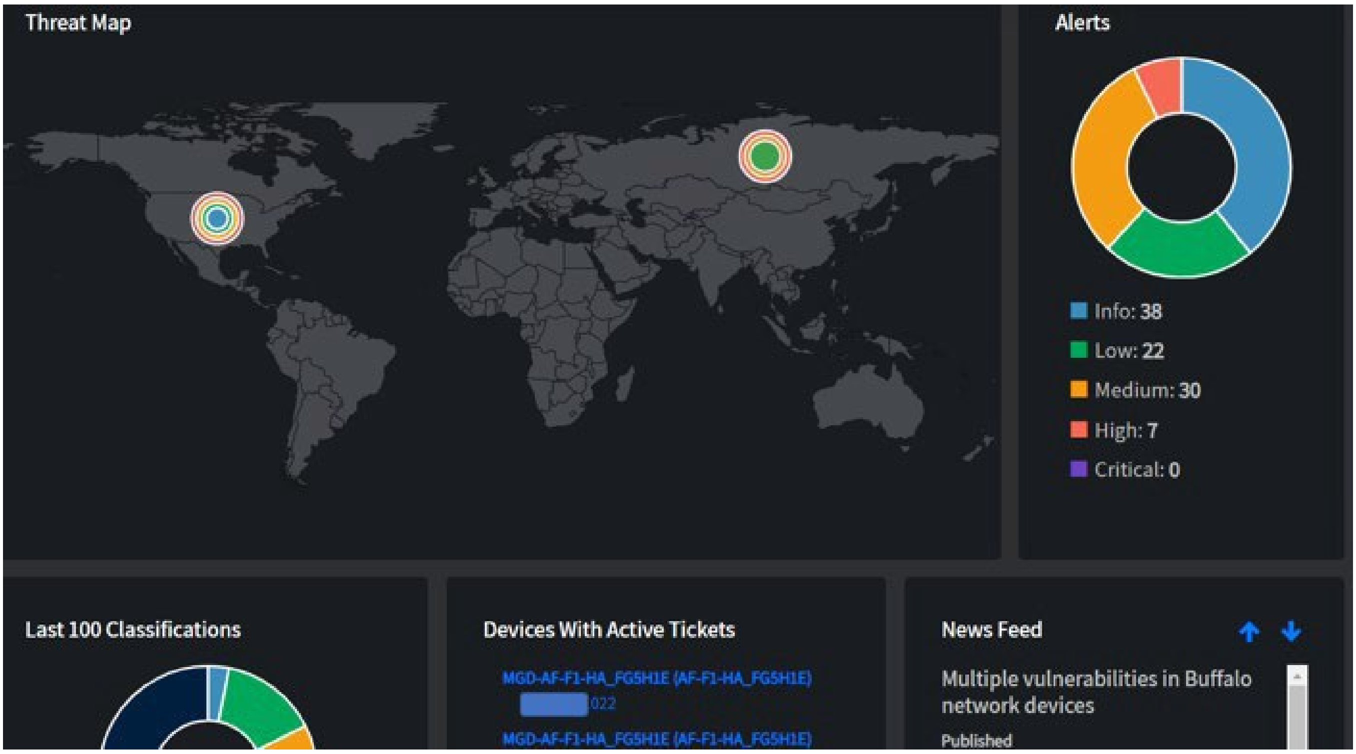


Figure 6: Lightning Portal Dashboard

Dashboard > Threat Map

The Threat Map displays the region of origin associated with security [incidents](#) generated. The color of the dot represents the severity of the incident, and the size of the dot represents the number of incidents.

Figure 7: Dashboard > Threat Map

For more detailed incident information, select the dot of interest to open the full [incident](#) report (see example in Figure 8 below).

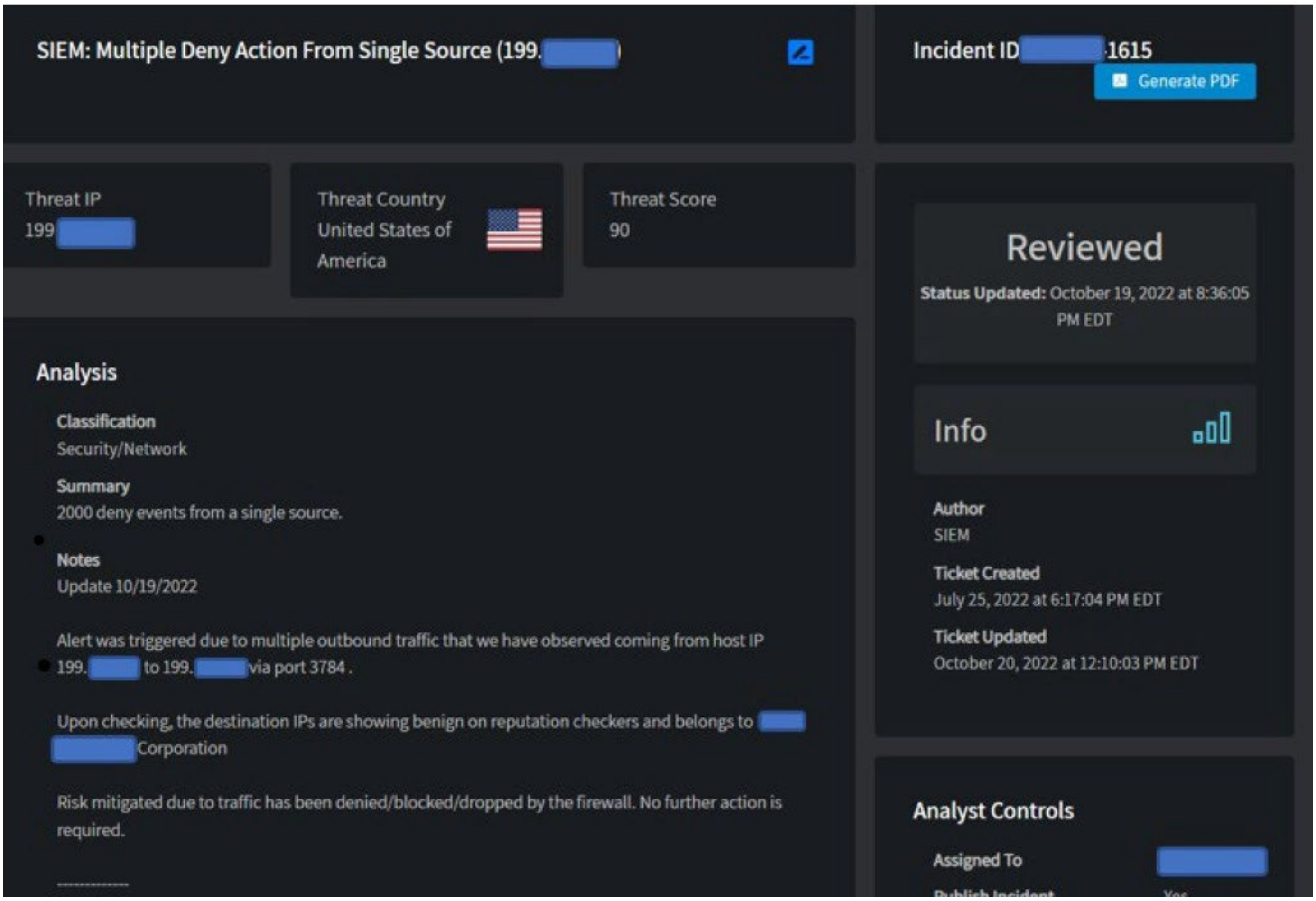


Figure 8: *Incident Report*

Dashboard > Alerts Widget

The Alerts widget displays a pie chart representation of the current collection of active incidents, divided into levels of severity. Select any section of the chart to generate a List of Incidents for a specific level of severity (see Figure 10 below).

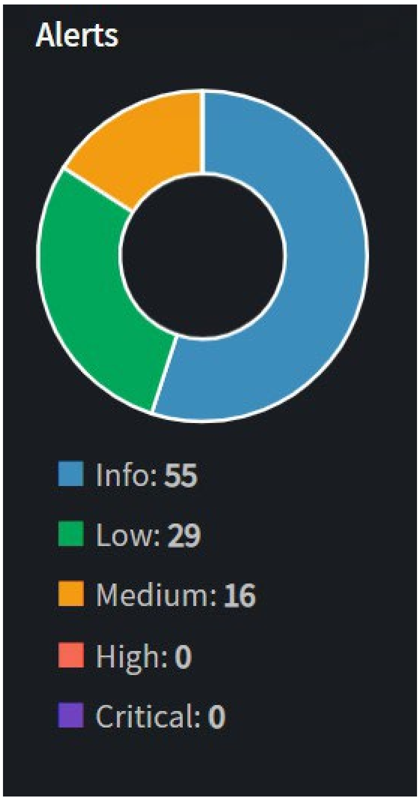
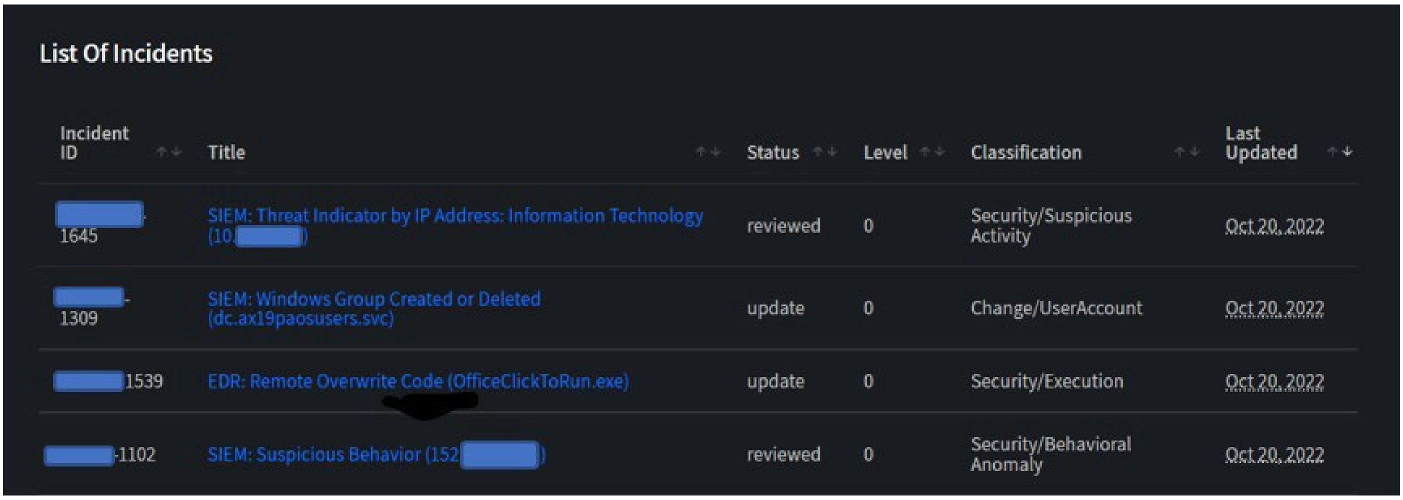


Figure 9: Alerts Widget

Incidents are predefined at the following levels:

- **Informational (0)** – Have <u>no impact</u> and are intended to track activity. Examples: false positives, approved scanning vendors, test alerts.
- **Low (1)** – May have <u>little impact</u> and are mostly alerts to provide information. Examples: login or logout notifications, failed login notifications, application or system update notifications, application or system error messages.
- **Medium (2)** – May have a <u>medium level of impact</u> on the network or system and could lead to unnecessary leakage of information or exposure of vulnerabilities Examples: port scans, vulnerability scans, social media traffic, unusual network traffic, multiple failed logins.
- **High (3)** – May have a <u>high level of impact</u> on the network or system and could lead to malware infection, data leakage, and disruption of operations due to network or system down time. Examples: download of malicious software, leakage of file from internal network, DoS (denial of service) or DDoS, P2P traffic (torrent), cloud storage traffic, exploit launching.
- **Critical (4)** – May have a <u>severe level of impact</u> to the network or system and indicates a compromise. Examples: malware infection, backdoor or Trojan traffic, outbound DDoS, bot net traffic.

Note: Incident tickets are resolved based on the customer-defined SLAs (service level agreements) for each level of ticket.



List Of Incidents

Incident ID	Title	Status	Level	Classification	Last Updated
[redacted]-1645	SIEM: Threat Indicator by IP Address: Information Technology (10.[redacted])	reviewed	0	Security/Suspicious Activity	Oct 20, 2022
[redacted]-1309	SIEM: Windows Group Created or Deleted (dc.ax19paosusers.svc)	update	0	Change/UserAccount	Oct 20, 2022
[redacted]1539	EDR: Remote Overwrite Code (OfficeClickToRun.exe)	update	0	Security/Execution	Oct 20, 2022
[redacted]-1102	SIEM: Suspicious Behavior (152[redacted])	reviewed	0	Security/Behavioral Anomaly	Oct 20, 2022

Figure 10: List of Incidents

Dashboard > Last 100 Classifications Widget

The Last 100 Classifications widget displays a pie chart representation of the 100 most recent incidents, divided by classification status. Select any section of the chart to generate a list of incidents of the desired classification status (similar to Figure 10 above).

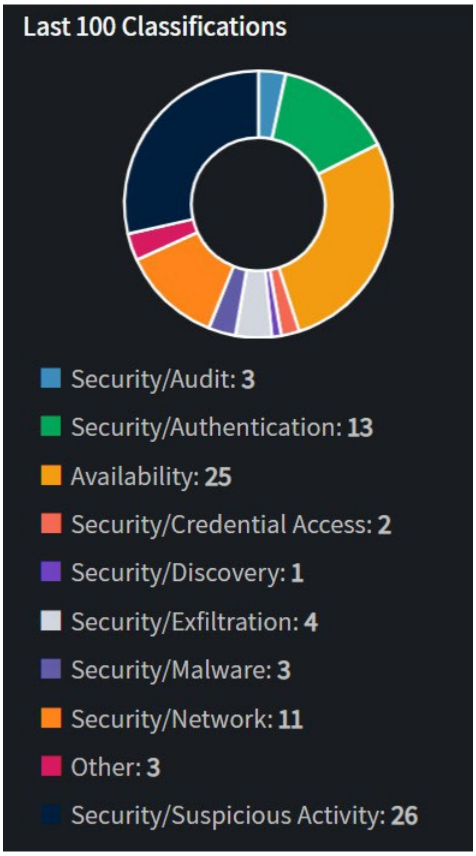


Figure 11: Last 100 Classifications Widget

Dashboard > Devices with Active Tickets Widget

Figure 12: Devices with Active Tickets Widget

The Devices with Active Tickets widget provides a list of devices attached to an active ticket. Click the first, bolded line to open a detailed device information screen (see Figure 13 below). Click the second line to open the detailed incident report including the listed device (see Figure 14 below).

Figure 13: Detailed Device Information Screen

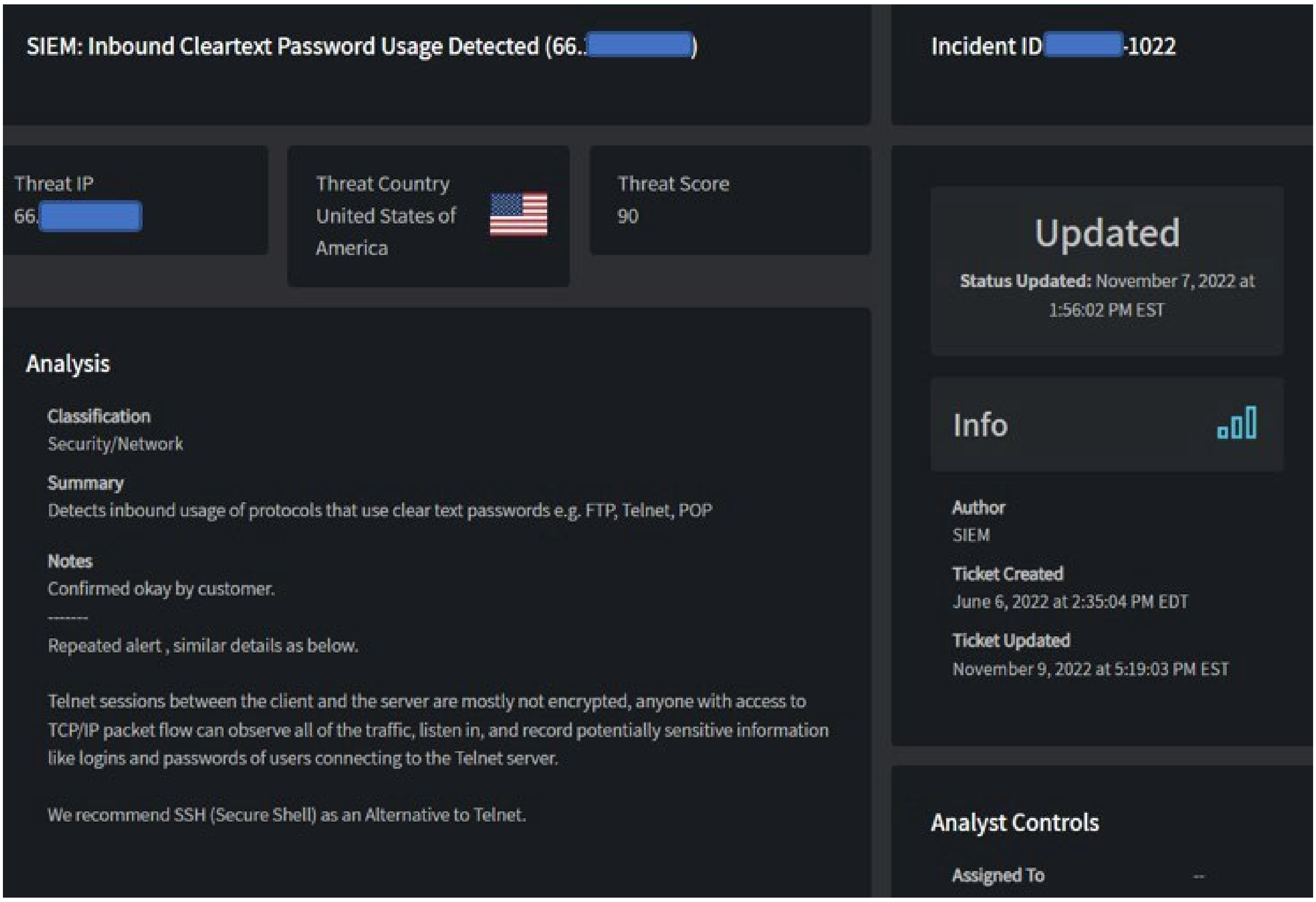


Figure 14: Detailed Incident Report

Dashboard > News Feed Widget

The News Feed widget provides recent security news from trusted and well-known sources.

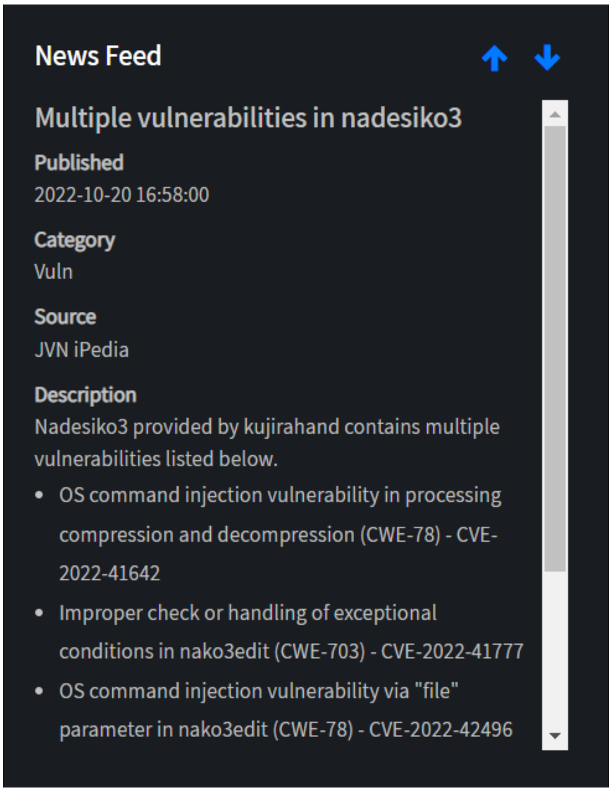
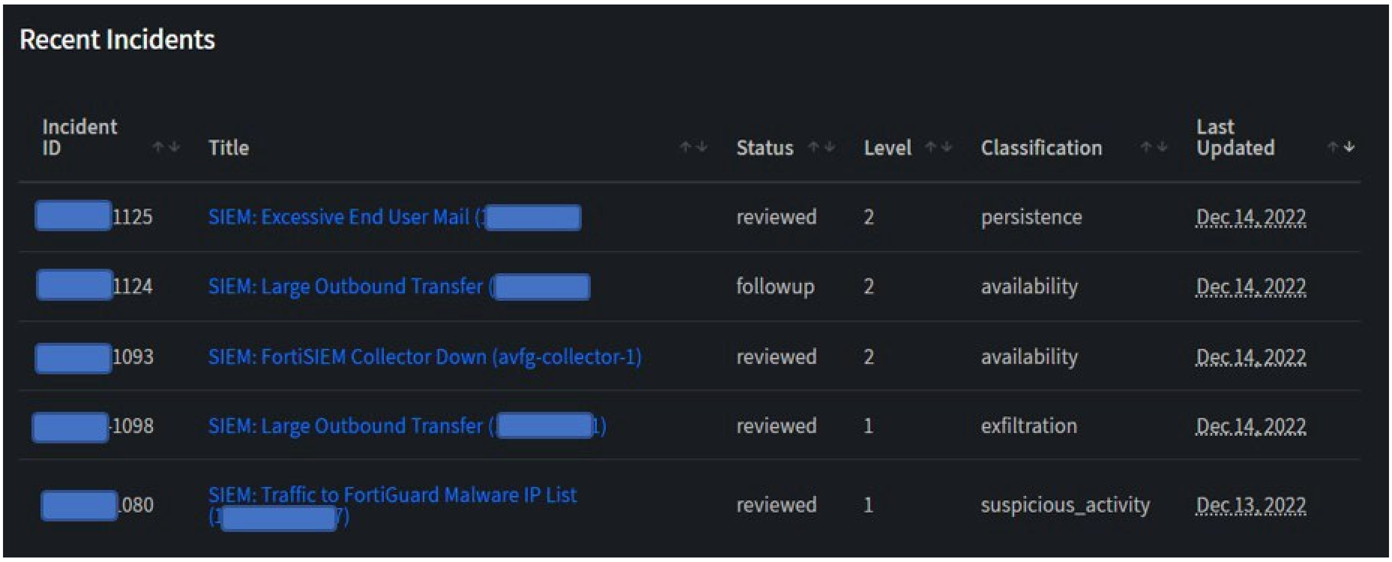


Figure 15: News Feed Widget Display

Dashboard > Recent Incidents

The Recent Incidents widget is at the bottom of the Dashboard and provides a list of the five most recently updated incidents.



Recent Incidents

Incident ID	Title	Status	Level	Classification	Last Updated
[redacted]1125	SIEM: Excessive End User Mail ([redacted]	reviewed	2	persistence	Dec 14, 2022
[redacted]1124	SIEM: Large Outbound Transfer ([redacted]	followup	2	availability	Dec 14, 2022
[redacted]1093	SIEM: FortiSIEM Collector Down (avfg-collector-1)	reviewed	2	availability	Dec 14, 2022
[redacted]1098	SIEM: Large Outbound Transfer ([redacted]1)	reviewed	1	exfiltration	Dec 14, 2022
[redacted]080	SIEM: Traffic to FortiGuard Malware IP List ([redacted]7)	reviewed	1	suspicious_activity	Dec 13, 2022

Side Navigation Bar

The Side Navigation Bar is comprised of the following menu options which allow the user to navigate to different functions within the Lightning Portal.

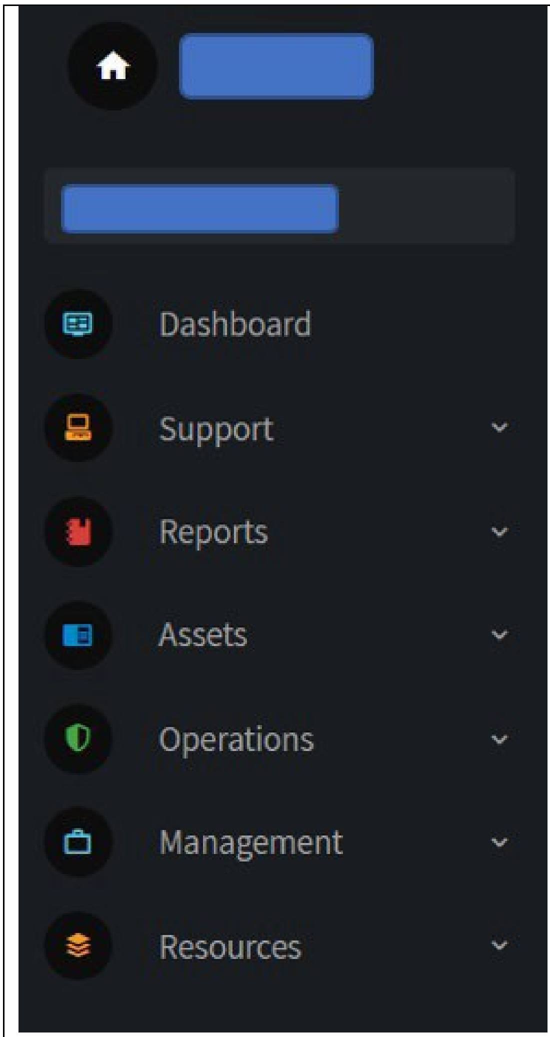


Figure 16: Side Navigation Bar

1. **Dashboard**: Opens the Dashboard view from any page.
2. **Support**: Includes functions relating to: support tickets, incidents, file repository, library and news feed.
3. **Reports**: Opens the Report Builder and scheduled reports.
4. **Assets**: Manage users, contacts, devices, agents, and groups.
5. **Operations**: Access response plans and bulletins.
6. **Management**: Access notifications, audits and session tracking.
7. **Resources**: Access downloads.

Support

The Support menu provides navigation options to review support tickets, incidents, upload files, access the library and view the News Feed.

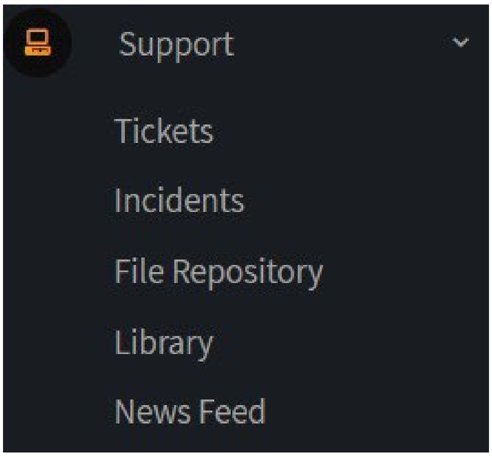


Figure 17: Support Menu

Support > Tickets

In the Lightning Portal, support requests are submitted and viewed via the Support Tickets function. The Lightning Portal contains three options for finding/viewing support ticket information:

1. Ticket Search: Search for a support ticket using a variety of search criteria.
2. Ticket Lookup: View detailed support ticket information by entering a specific Ticket ID.
3. List of tickets: View a list of support tickets sorted by any of the columns in the table.

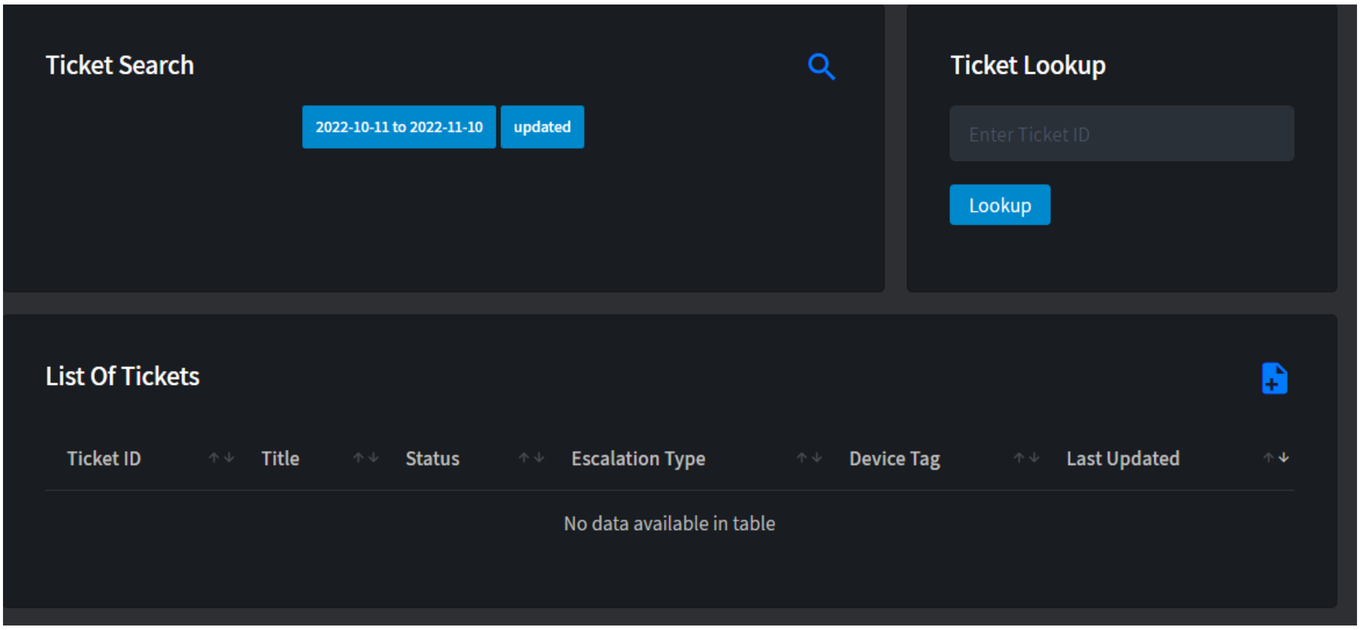


Figure 18: Support > Tickets Functionality

Support Ticket Search

To begin a search using the Ticket Search feature, select the Search icon . The Ticket Search criteria window will display the following options (see Figure 19)

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Device Tag	Search support tickets for a specific device only
Date Range	Select the date range for the search
Date Type	Select Created, Updated or Both
Status	Select Status (Request, Open, Reviewed, Updated, Customer Response, Analyst Follow-Up, Closed)
Search Notes	Use this option to search support ticket notes by keywords.

Note: These fields are not required so only enter information in the fields to be searched.

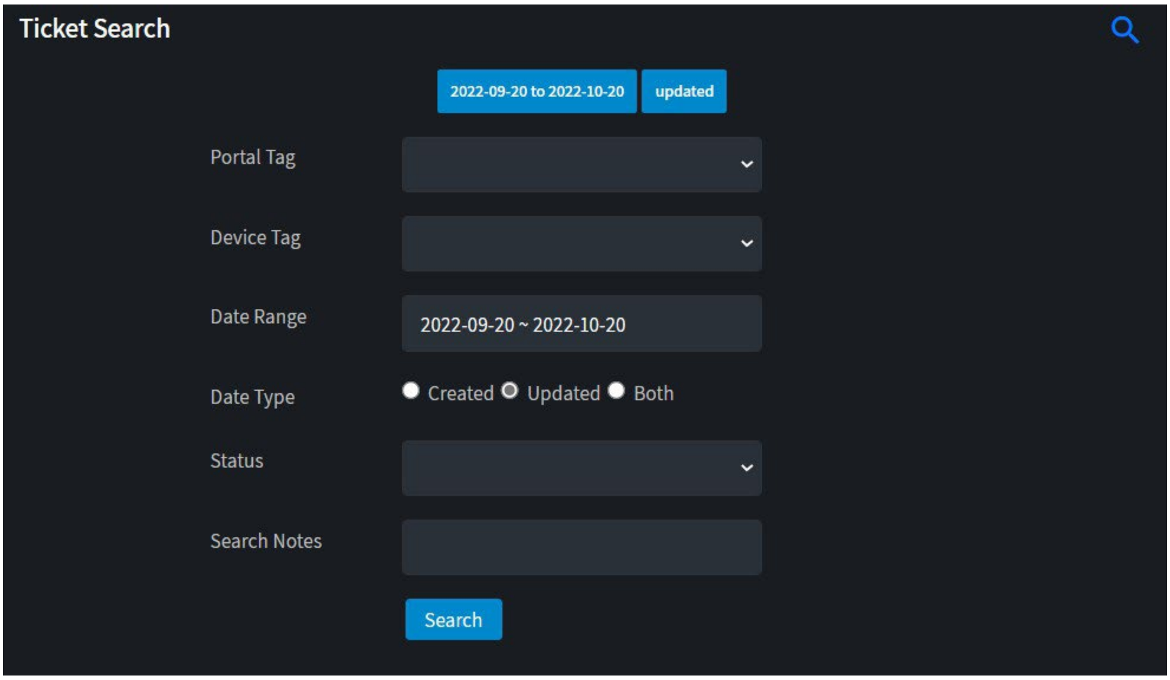


Figure 19: Ticket Search Feature

Select the Search button to run the search with the desired criteria defined. When the search is complete, the results will display in the List of Tickets section of the screen.

Note: The List of Tickets section will always reflect the search criteria displayed in the blue boxes in the Ticket Search section.

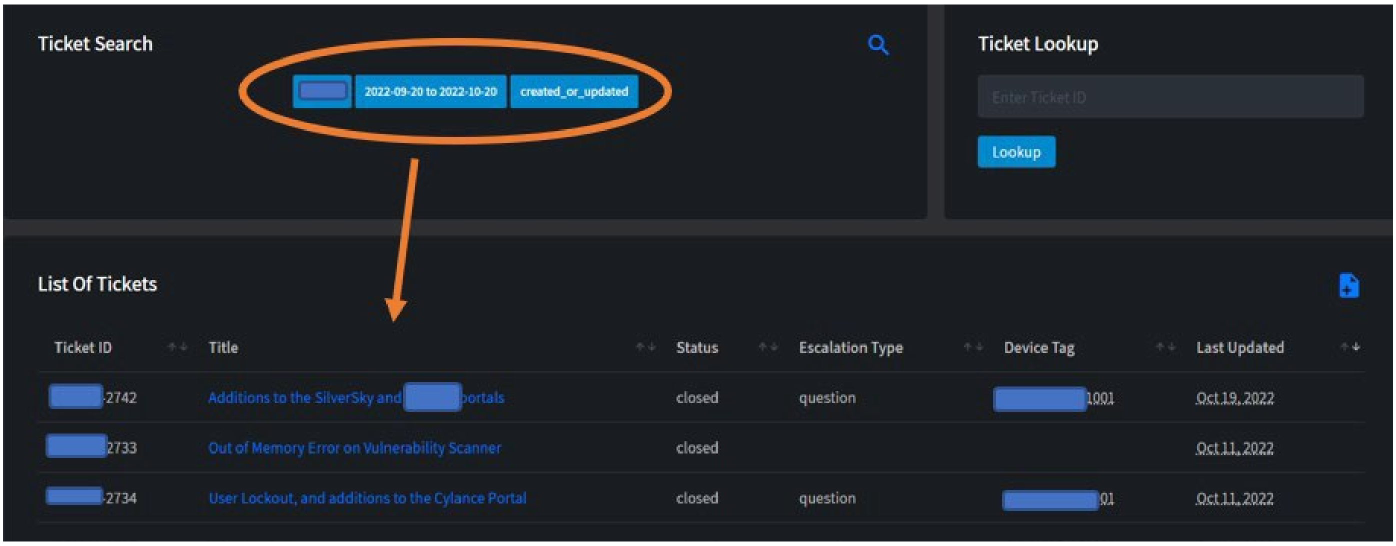


Figure 20: List of Tickets Search Results

Ticket Lookup

An additional option is to search for a ticket using the Ticket ID via the Ticket Lookup feature. Enter the full Ticket ID and then select Lookup.

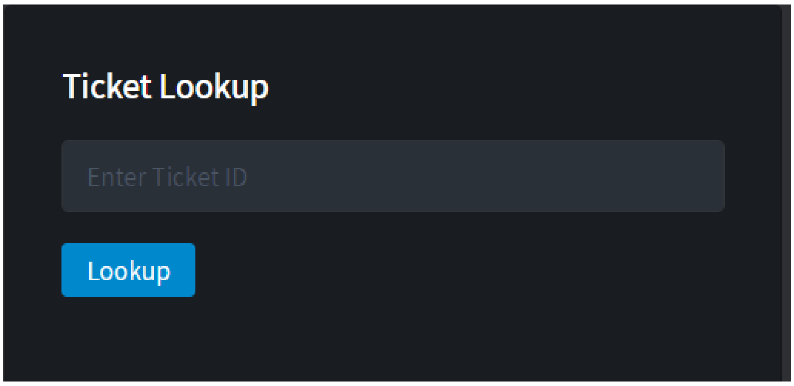


Figure 21: Ticket Lookup Feature

List of Tickets

The List of Tickets feature provides a listing of support tickets with the default sorting configuration of the most recently updated tickets at the top. To sort ascending/descending using any of the data fields in the table, select the up/down arrows next to the column headings.

Note: The default List of Tickets contains a list of tickets updated within the past month as can be seen in the Ticket Search section.

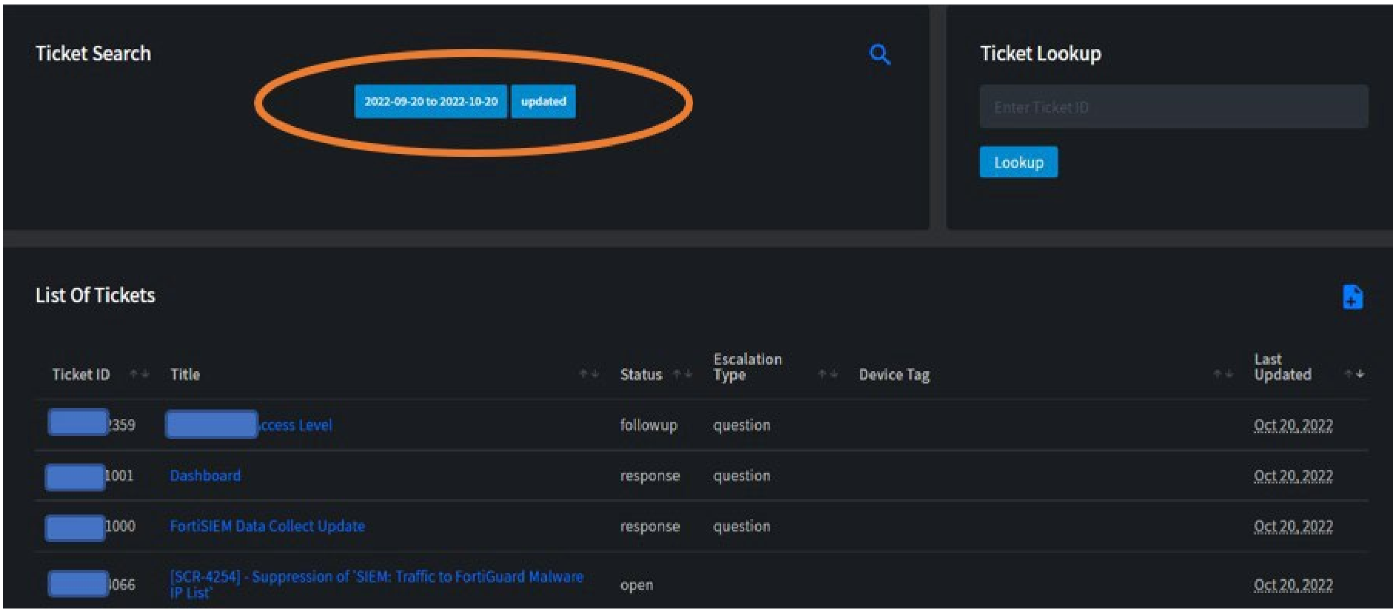


Figure 22: Ticket Screen Showing Search Criteria

Create a ticket

To create a new support ticket, select the Create Ticket icon from the top right corner of the List of Tickets section.

SILVERSKY

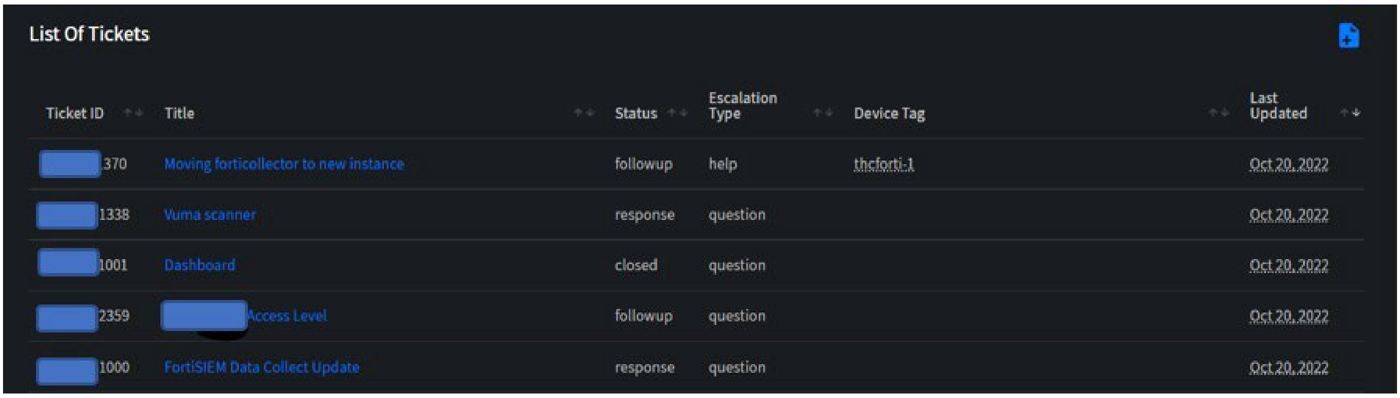


Figure 23: Ticket Information Screen

Enter the required information in the New Ticket screen (see Figure 24 below):

Data Field	Description
Title	Provide a descriptive title for the support ticket (ex: John Smith Access Level Change Request)
Escalation Type	Select the escalation type from the drop-down box. Options include: 1. General Question 2. Log Request 3. Investigation Help 4. Sales Inquiry 5. Service Feedback
Summary	Add a detailed summary of any applicable information regarding the topic of the support ticket.
Device	If the support ticket is specific to a device, select the device name from the drop-down.
Assigned	There is no need to populate this field, as it will be completed by the SOC team upon receipt of the support ticket.
Notifications	Select which Contacts should receive email alerts regarding this ticket. To choose multiple contacts hold the CTRL button when making selections.

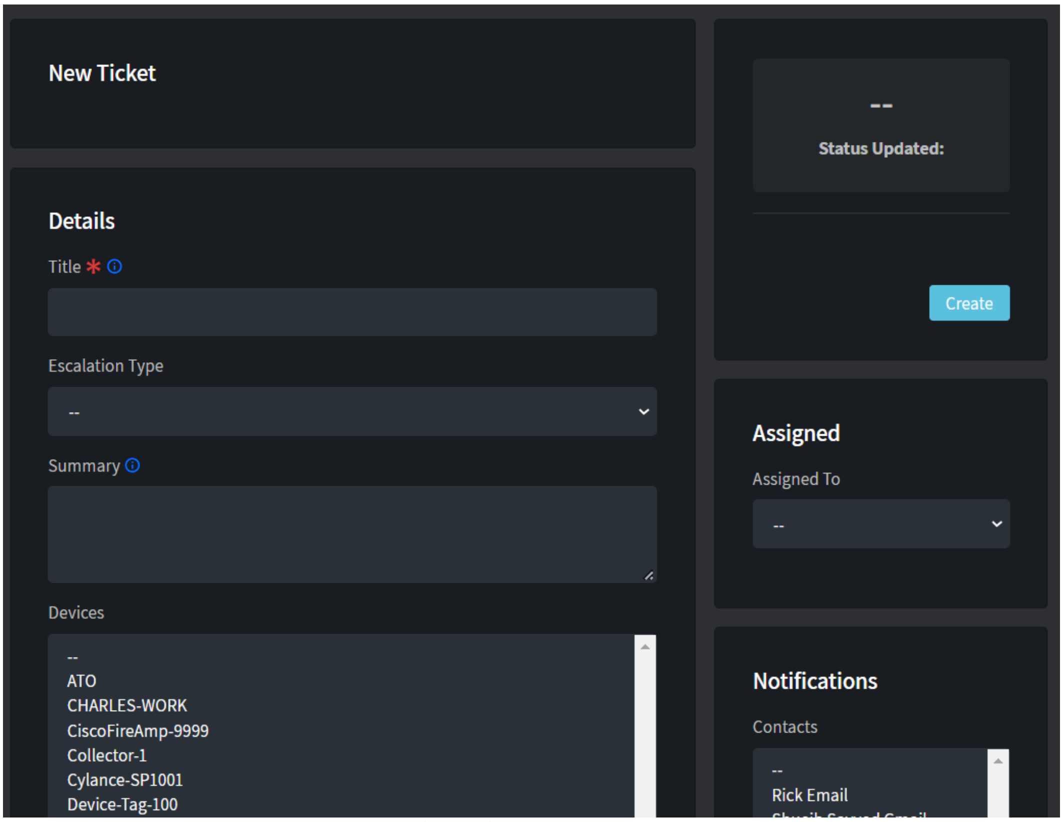


Figure 24: Create New Ticket Screen

Select Create to submit the new ticket request. Upon submission, a Ticket ID will be assigned:

Figure 25: Ticket Submission Confirmation

All communications regarding support tickets will be accessible in the Lightning Portal. Also, update notifications will be sent to the designed Contact(s) on the support ticket via email to keep Contacts informed when tickets are updated. The email will originate from notifier@outsoc.com, and it is recommended to add this email address to the safe list in the email client. See the sample email notification in Figure 26 below.

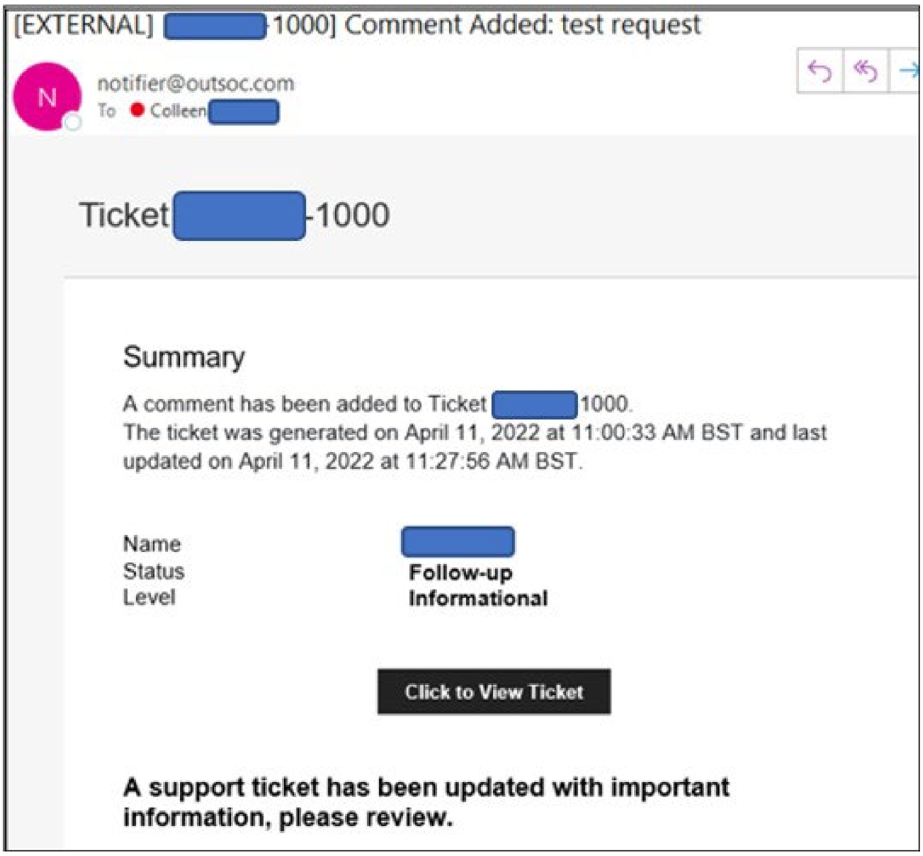


Figure 26: Sample Notification Email

Select the link in the email message to view the ticket. Note: this is a time sensitive link that is view-only. To edit/update the support ticket, a User must login to the Lightning Portal .

Support > Incidents

Security incidents are events that have been flagged as a potential security threat. The Incident functionality in the Lightning Portal allows SOC personnel and Users to view and update security incidents (see Figure 27 below).

Note: all incidents are published in the Lightning Portal, but not all incidents will create an email notification to a Contact. Notification settings are determined by the Playbook setup in the Contacts functionality.

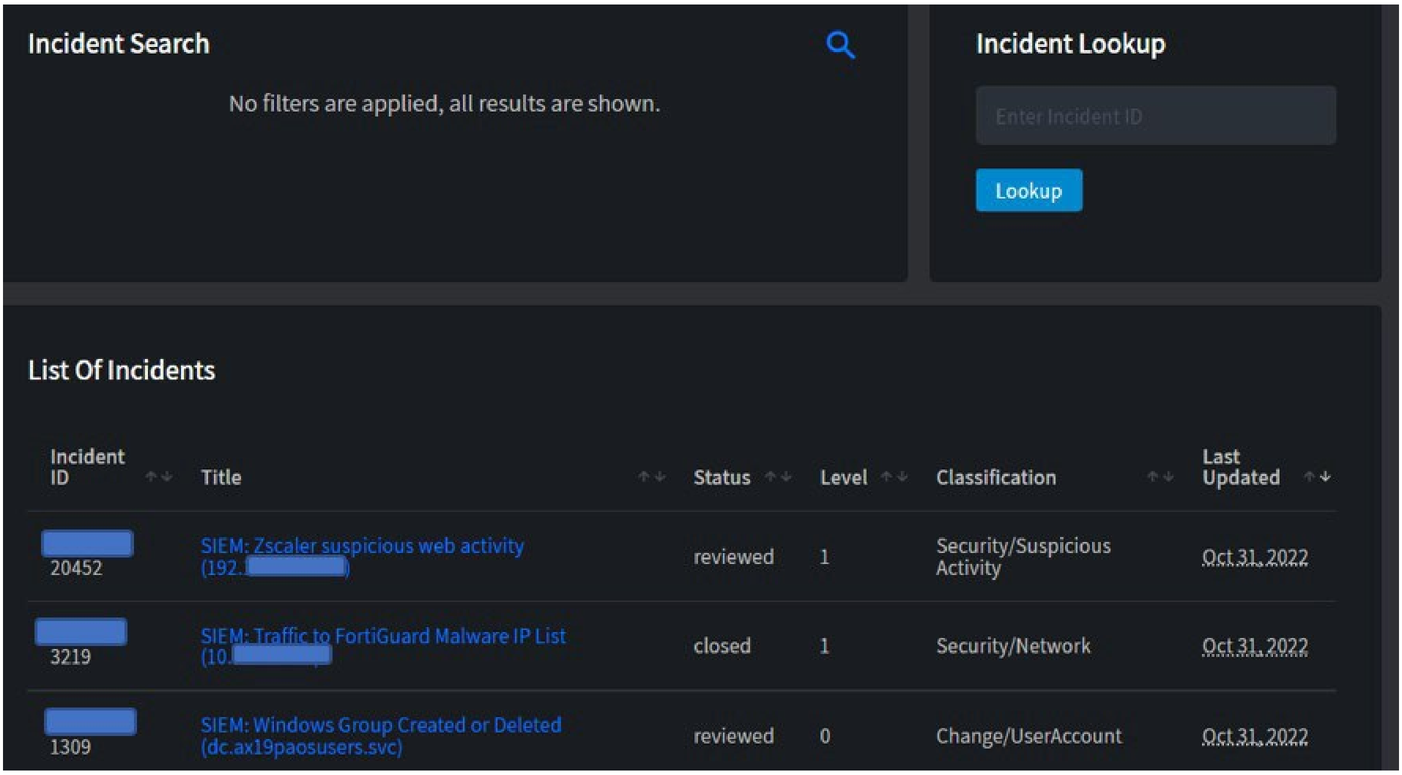


Figure 27: Incident Screen

Incident search

All incident tickets can be searched via the Incident Search functionality. Select the search icon to populate search criteria.

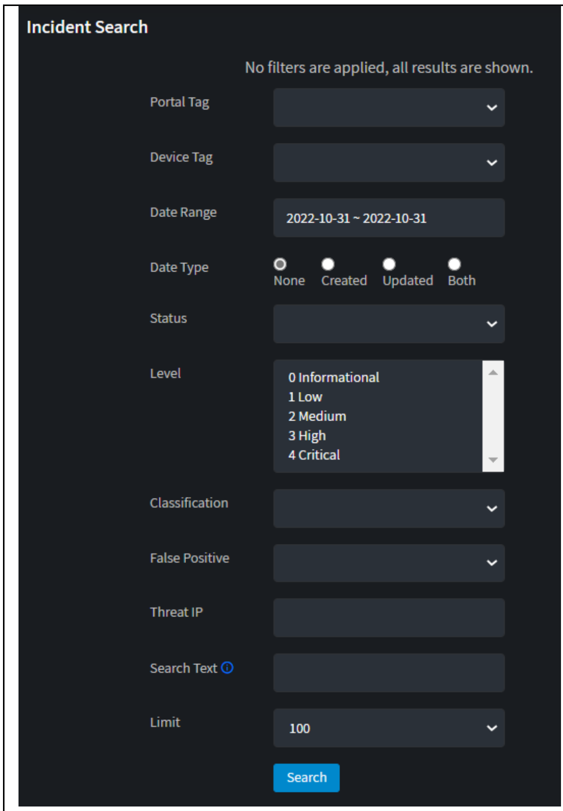


Figure 28: Incident Search Criteria

1. **Portal Tag:** Select the Portal Tag to search from the drop-down list.
2. **Device Tag:** Select a device from the list to view only incidents for a specific device.
3. **Date Range:** Select the date range to search.
4. **Date Type:** Select the date created, date updated or both to narrow the search.
5. **Status:** Select the status of incidents to search (Open, Active, Reviewed, Updated, Customer Response, Analyst Follow Up, Pending, Closed). If left blank, the search will include all status options.
6. **Level:** Select the incident level to search (0 - Informative, 1 - Low, 2 - Medium, 3 – High, 4-Critical). Note: each incident level has a response time indicated in the Service Level Agreement (SLA).
7. **Classification**: Type of threat, NIST threat classification
8. **False Positive**: Whether the incident has been marked as a tuning opportunity (noise to filter, or of low security value to suppress or modify).
9. **Threat IP**: The source address parsed from any threat (ex: attacker IP or scan origin)
10. **Search Text:** Use this option to search by keywords.
11. **Limit:** Define the maximum number of records to return.

Note: These fields are not required so only enter information in the fields to be searched.

An additional search option is to search for an incident via the Incident Lookup feature on right. Enter the Incident ID, then select Lookup. Note: the complete Incident ID is required.

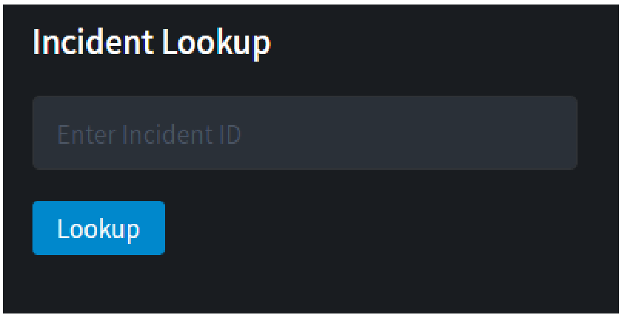
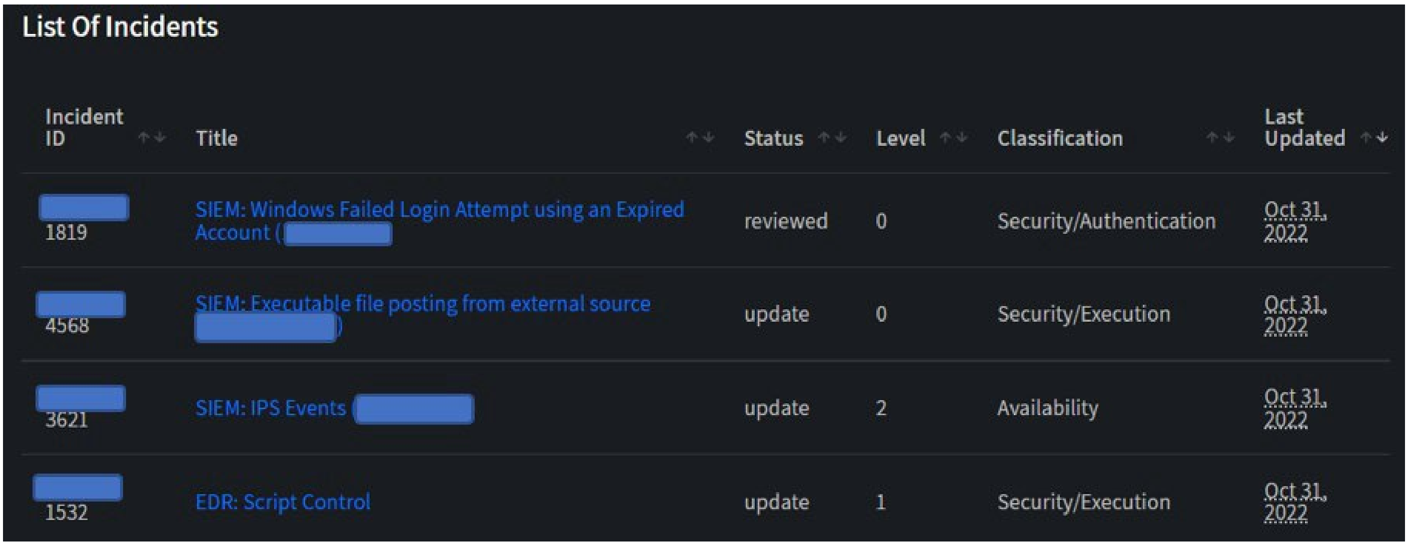


Figure 29: Incident Lookup Feature

List of Incidents

The List of Incidents by default displays the 100 most recent incidents sorted by the Last Updated column (see Figure 30 below). The arrows near each column header can be used to sort incidents accordingly. The column headings include:

Data Field	Description
Incident ID	System-generated unique identifier to be referenced in any communication regarding the incident
Incident Title	Descriptive title to communicate basic incident facts
Status	Displays the status of the incident, including the following: • **Active**: Includes all tickets in the Analyst Follow-up, Updated, and Reviewed statuses. • **Open**: a new incident, queued for analyst review. • **Reviewed**: the analyst investigation is complete, and the incident is pending review from the customer (before manual or automatic closure). • **Updated**: a previously Reviewed or Closed incident has been updated with new alerts, pending an analyst's investigation and update. • **Customer Response**: an incident queued for an analyst to reply to a customer comment • **Analyst Follow-Up**: An analyst has replied to a customer comment and is waiting on a follow-up. • **Pending**: an incident in a paused/holding state. • **Closed**: following seven days of no updates, Reviewed incidents are automatically set to Closed, or a customer can manually set an incident to Closed if desired.
Level	• **Informational (0)** – Have no impact and are intended to track activity. Examples: false positives, approved scanning vendors, test alerts. • **Low (1)** – May have little impact and are mostly alerts to provide information. Examples: login or logout notifications, failed login notifications, application or system update notifications, application or system error messages. • **Medium (2)** – May have a medium level of impact on the network or system and could lead to unnecessary leakage of information or exposure of vulnerabilities Examples: port scans, vulnerability scans, social media traffic, unusual network traffic, multiple failed logins. • **High (3)** – May have a high level of impact on the network or system and could lead to malware infection, data leakage, and disruption of operations due to network or system down time. Examples: download of malicious software, leakage of file from internal network, DoS (denial of service) or DDoS, P2P traffic (torrent), cloud storage traffic, exploit launching. • **Critical (4)** – May have a severe level of impact to the network or system and indicates a compromise. Examples: malware infection, backdoor or Trojan traffic, outbound DDoS, bot net traffic.
Classification	Defined by the SOC team during analysis, the type of threat, NIST style classification.
Last updated	Timestamp of the most recent incident update



List Of Incidents

Incident ID	Title	Status	Level	Classification	Last Updated
[redacted] 1819	SIEM: Windows Failed Login Attempt using an Expired Account ([redacted]	reviewed	0	Security/Authentication	Oct 31, 2022
[redacted] 4568	SIEM: Executable file posting from external source [redacted])	update	0	Security/Execution	Oct 31, 2022
[redacted] 3621	SIEM: IPS Events ([redacted]	update	2	Availability	Oct 31, 2022
[redacted] 1532	EDR: Script Control	update	1	Security/Execution	Oct 31, 2022

Figure 30: List of Incidents

Incident Detail View

To view detailed information about an incident, select the hyperlinked Title in the List of Incidents. A new window will open displaying full details of the incident (see Figures 31 and 32 below). Key information found in the detailed incident report includes:

Sections	Section Description
Threat Score	Displays a system-generated score estimating the potential security risk. The range is from 0-100 with higher numbers indicating a greater threat.
Analysis	Displays analysis information provided by a SOC analyst.
Details	Displays a summary of devices and events associated with the incident. Select the Expand icon to toggle to more detailed device and event information.
Recent Alerts	Displays recent alerts related to the incident.
Comments	This is where the SOC and the customer can have a conversation about an incident via comments.
Handling Notes	Displays summary notes created and managed by the SOC which are relevant to the incident. Notes may include specific handling instructions (ex: always check for hits in more than one threat service) or more general information (ex: customer is undergoing a pen test in December, please escalate all scan activity regardless of risk).
Notifications	Displays recent incident notification information sent to Contacts
Attachments	Provides access to attachments related to the incident.

The top section of the Detailed Incident window shows a summary of the threat details and analysis from the SOC team (see Figure 31 below). Note: In Figure 31 below, the Author of "SIEM" denotes the incident was created from the logs ingested by customer devices.

SILVERSKY

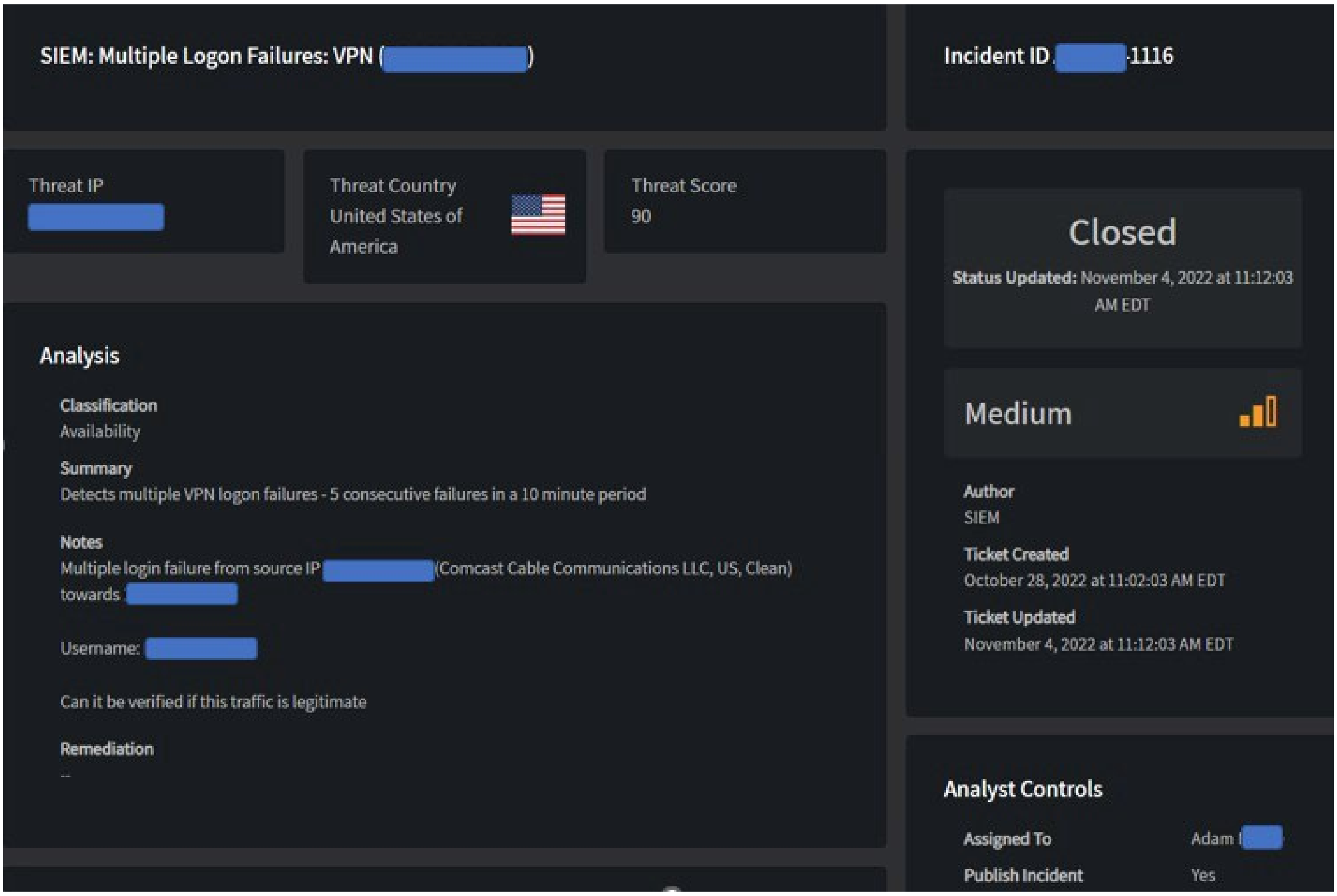


Figure 31: Incident Detail View (top half)

The bottom half of the Incident Detail window displays the handling notes, notifications, device details, recent alerts, and attachments (see Figure 32 below).

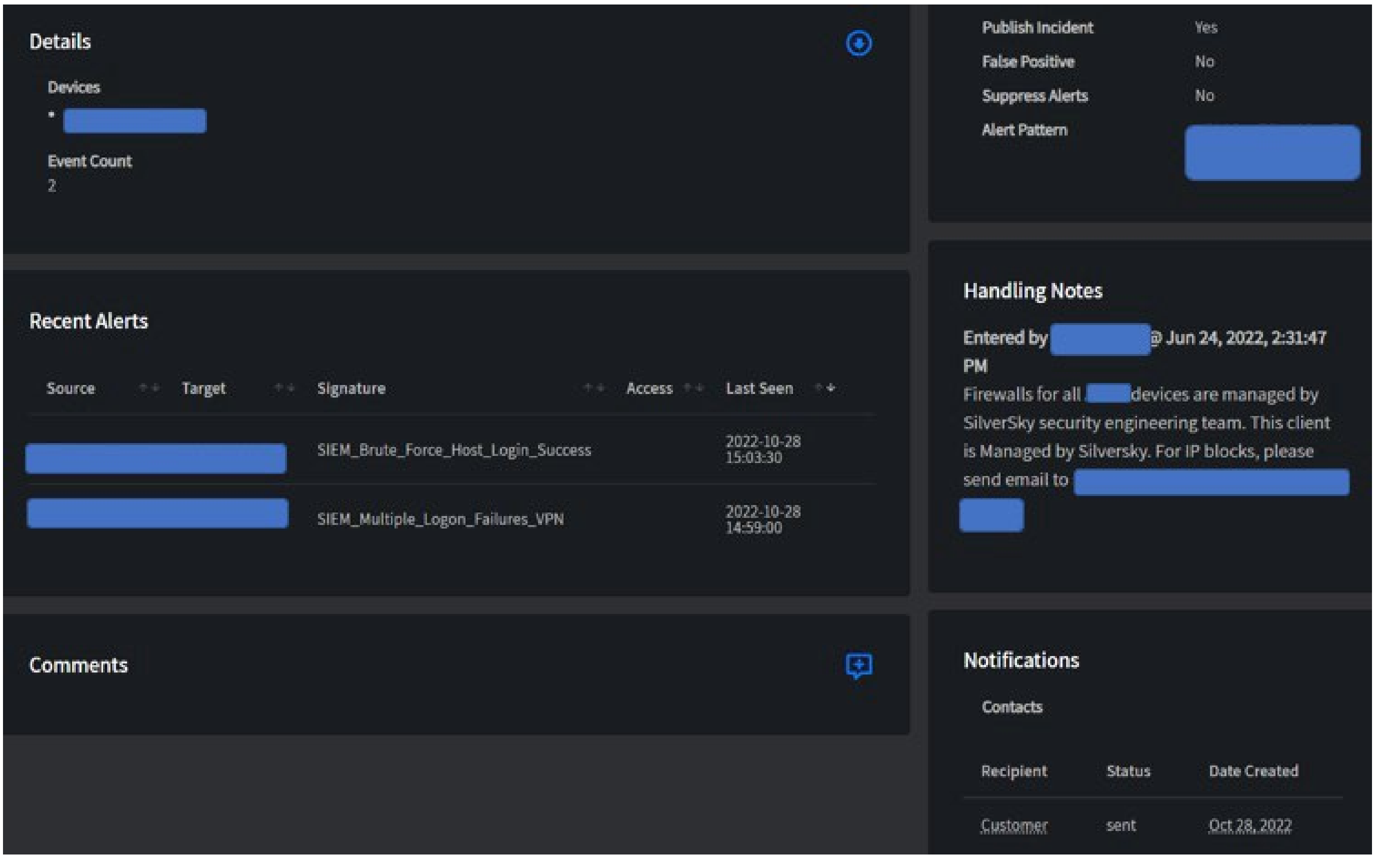


Figure 32: Incident Detail View (bottom half)

At the very bottom of the incident detail view is an area where comments and responses can be added by selecting the Add Comment icon to the right. When the comment is complete, select Save (see Figure 33 below), and the incident ticket will be updated. Note: responses/comments to an incident will generate an email notification to the Contact, if designated as such in the Playbook.

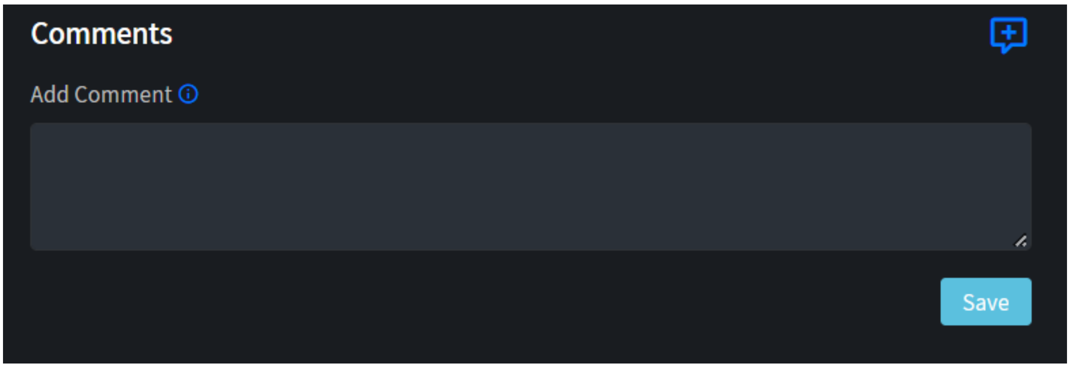


Figure 33: Incident Detail View > Save Comment

The details of the incident can be exported using the Generate PDF button (see Figure 34 below).

Figure 34: Generate PDF button

A detailed incident report will be created in PDF format (see Figure 35 below).

[[redacted]-3219] SIEM: Traffic to FortiGuard Malware IP [redacted])

INCIDENT SUMMARY:
Detects network traffic to FortiGuard Blocked IP List

TECHNICAL DETAILS:

WHAT	Threat Name	SIEM: Traffic to FortiGuard Malware IP List (10[redacted])
	Level	1
	Alert Count	14
WHY	Signature	SIEM_Excessive_End_User_Mail SIEM_Traffic_to_FortiGuard_Malware_IP_List
WHEN	Timestamp	Date Created: August 3, 2022 at 8:25:05 AM EDT Last Updated: October 31, 2022 at 12:03:04 PM EDT
WHERE	Target	Reporting Devices: [redacted] Target IP: [redacted]3, [redacted]
WHO	Threat	Threat IP: [redacted] Threat Country: Private IP Address

For more details please refer to: https://platform.outsoc.com/soc/incident/929edc82-715d-4f19-88ea-f296378b4dc8

Figure 35: Sample PDF Incident Report

Incident Notifications

Depending on Playbook settings, when new incidents are created, updated or closed, an email notification can be sent to designated Contacts (see example in Figure 36 below). Notification settings can also be configured by incident severity.

Escalation and notification emails will originate from notifier@outsoc.com, and it is recommended to add this email address to the safe list in an email client. The notification email includes a time-sensitive link to view the incident directly. To comment or reply to an incident, a User must login to the Lightning Portal.

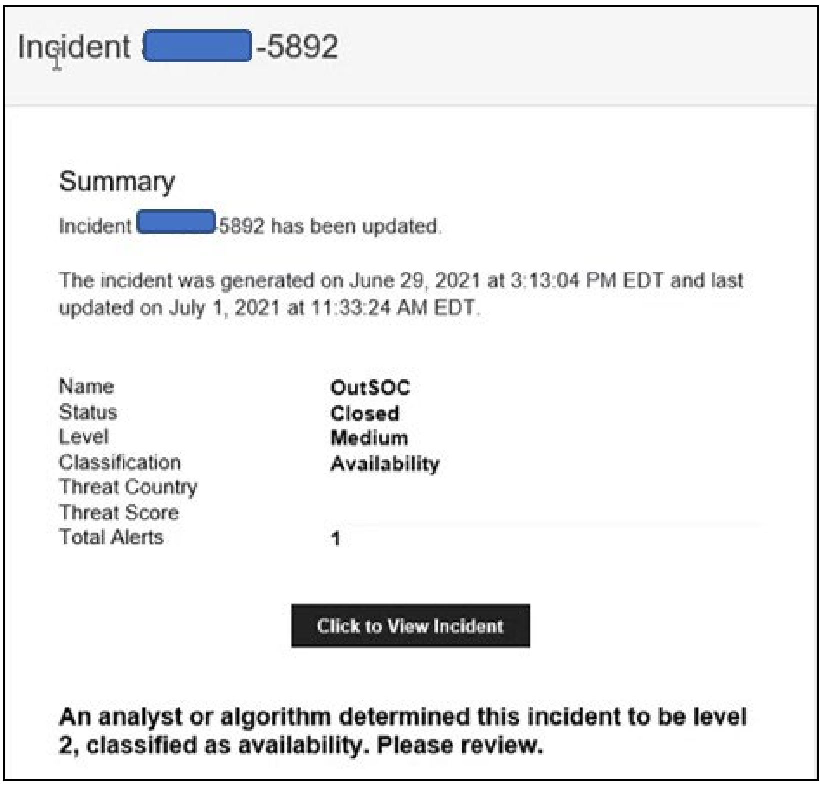


Figure 36: Incident Update Notification Email Example

Support > File Repository

The File Repository is a feature that allows users to securely upload and share files with other users and the SilverSky support and SOC teams. Often, files can be useful in communicating security issues, such as log files, screenshots, or files containing information about security threats.

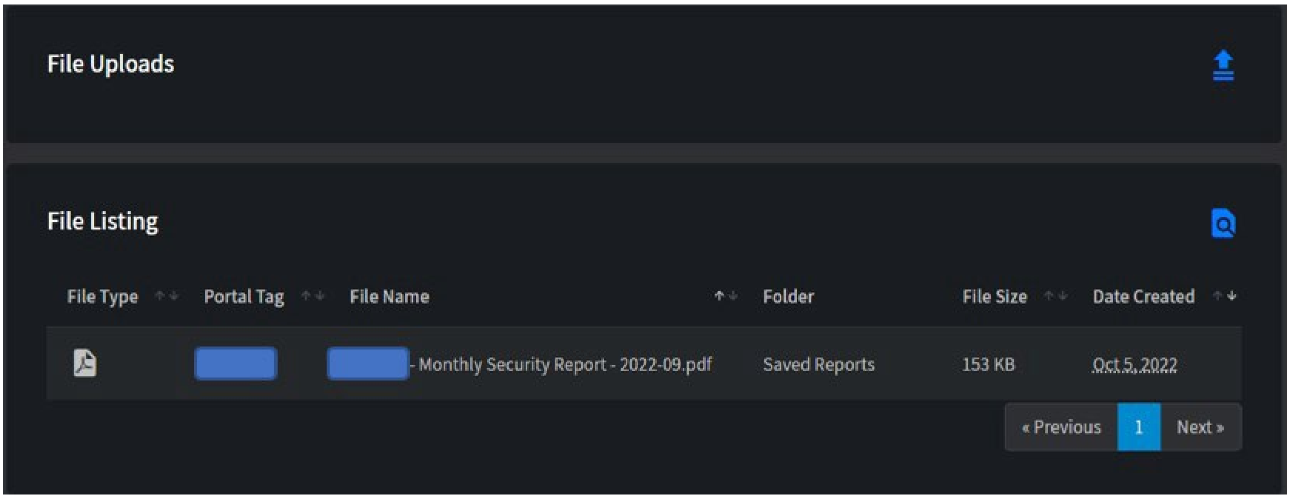


Figure 37: File Repository Feature

File Uploads

To upload a file, click the Expand icon on the File Uploads section to reveal upload options. Drag and drop the file or click in the box to navigate to the desired file. Designate where to store the new document in the File Repository by using the drop-down list (see Figure 38 below).

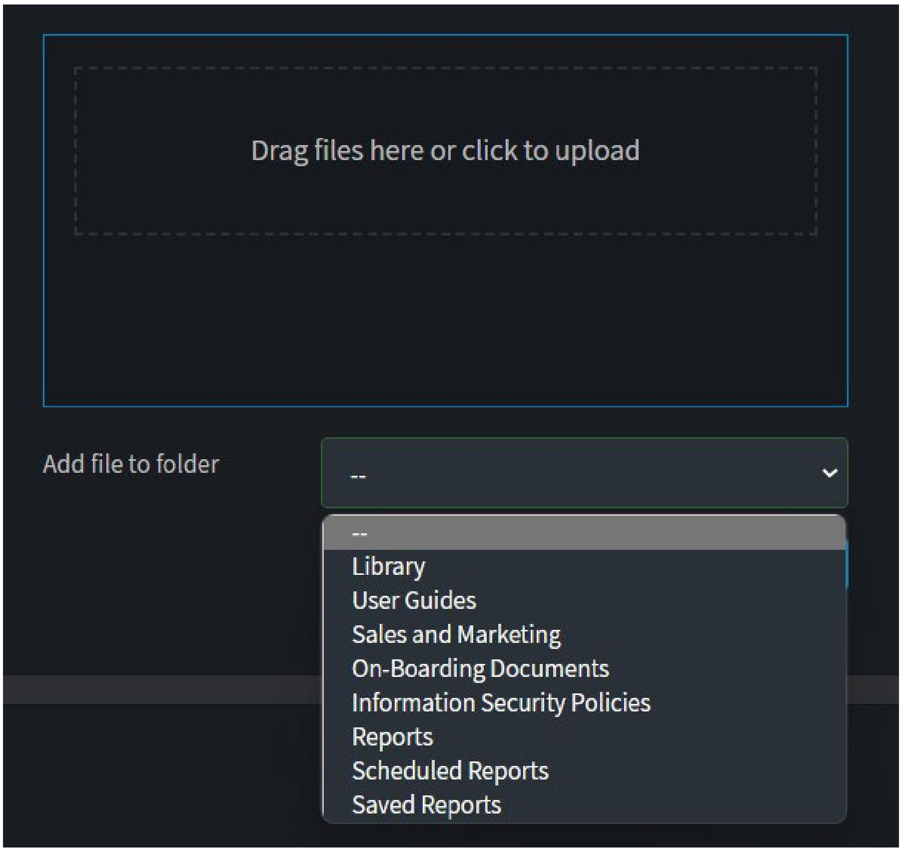


Figure 38: Upload File Feature

Guidelines for uploads include:

- Maximum file size supported is 100 MB
- Empty or zero byte files are not allowed
- The following file types are supported: bat, exe, cmd, sh, php, pl, cgi, 386, dll, com, torrent, js, app, jar, pif, vb, vbscript, wsf, asp, cer, csr, jsp, drv, sys, ade, adp, bas, chm, cpl, crt, csh, fxp, hlp, hta, inf, ins, isp, jse, htaccess, htpasswd, ksh, lnk, mdb, mde, mdt, mdw, msc, msi, msp, mst, ops, pcd, prg, reg, scr, sct, shb, shs, url, vbe, vbs, wsc, wsf, wsh

Select the Upload button when ready to upload the desired file.

View/Download/Edit/Delete a File

To view, download, edit or delete a file, navigate to the File Listing section. Select the file name to choose the entire row (see Figure 39 below).

SILVERSKY

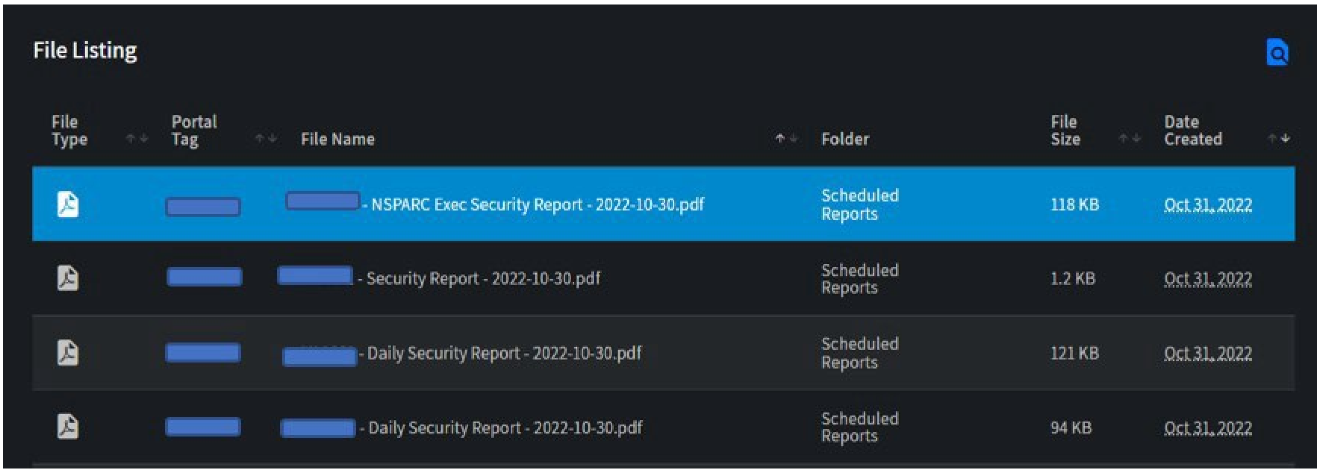


Figure 39: File Listing with Row Selected

Right click anywhere on the row and select an option.

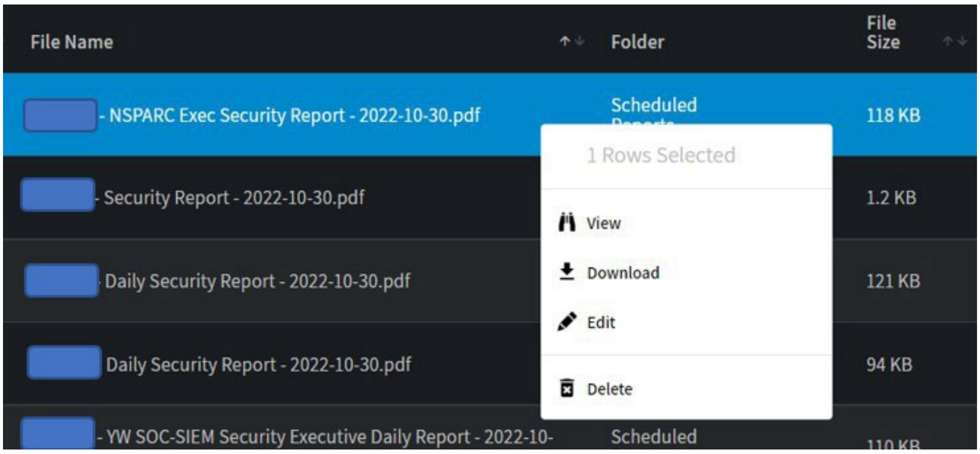


Figure 40: File Listing with Row Selection and Right Click Menu

Command	Functionality
View	Opens File Details window to view file attributes (see Figure 41 below).
Download	The file will be added to the Downloads folder on the browser. Select the file name to open the file.
Edit	Opens the Edit File window to allow editing of the File Description (see Figure 42 below).
Delete	Deletes the file from the File Repository.

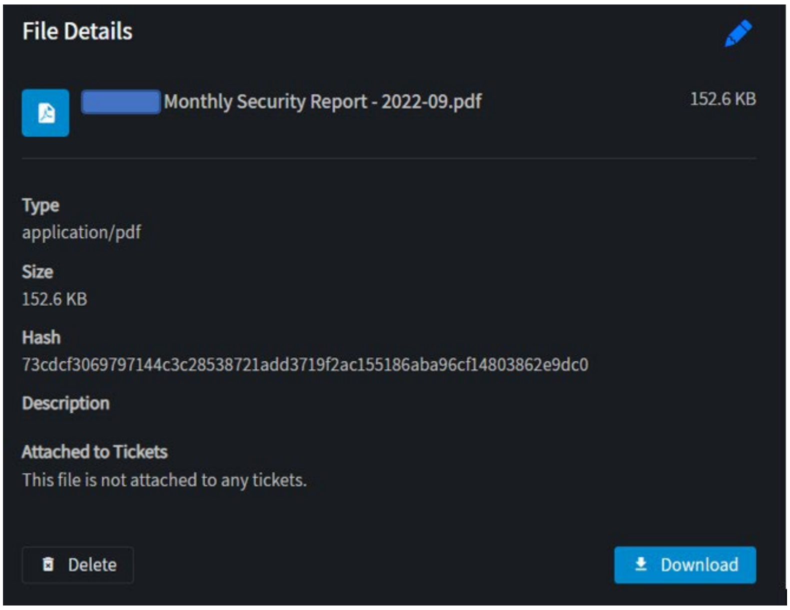


Figure 41: File Details Window

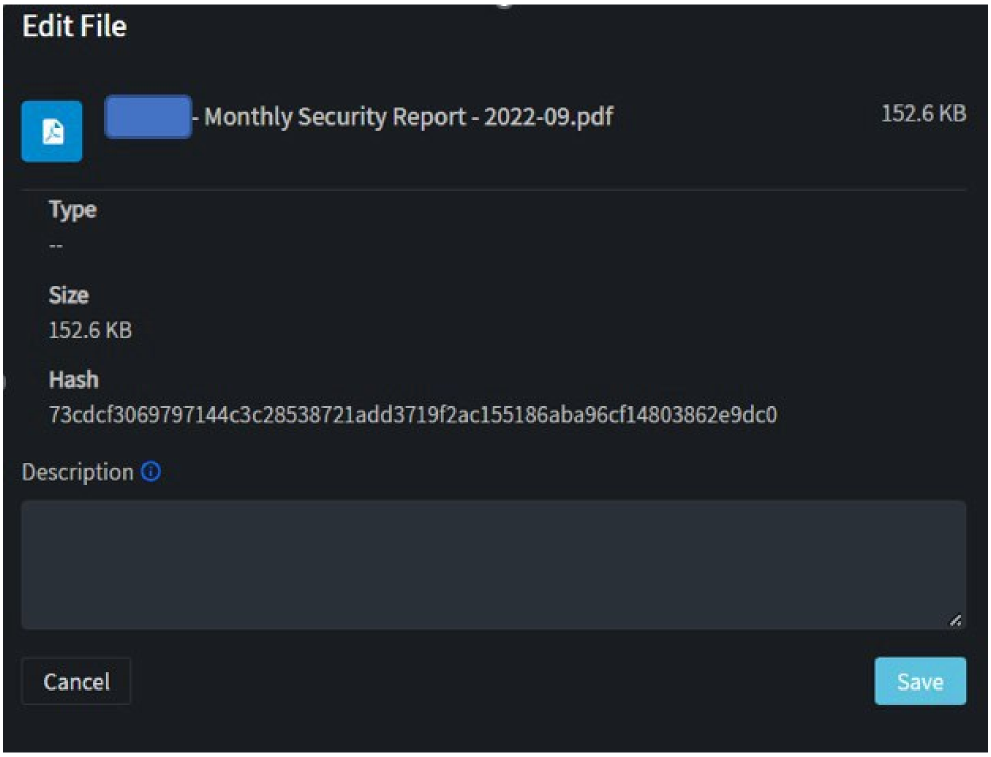


Figure 42: Edit File Description Window

Support > Library

The Library feature in the Lightning Portal provides a file structure to organize uploaded files and saved reports. Use the hyperlinks to navigate to the desired documents.

Figure 43: Library Feature

Support > News Feed

The News Feed functionality provides recent security news from trusted and well-known sources. The News Feed can be accessed via the [News Feed widget] on the Dashboard or from the Side Navigation Bar > Support > News Feed.

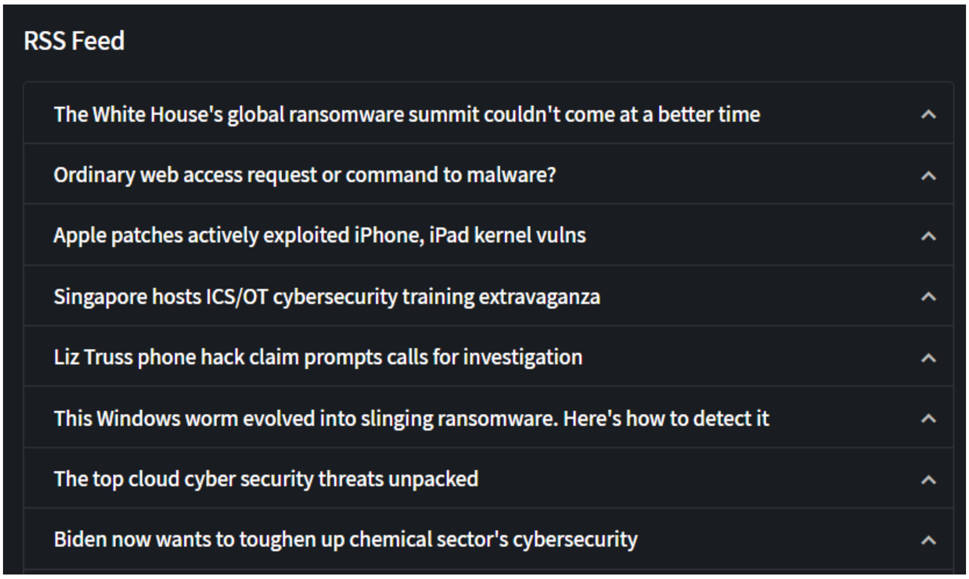


Figure 44: News Feed Feature

Reports

The Reports functionality can be accessed via the Side Navigation Bar and includes the options to build a report using the Report Builder tool or to use the List of Schedules which is a collection of scheduled report templates.

The Report Builder provides the ability to generate reports by utilizing a template or by building a custom report with desired criteria. The read-only Summary section on the right-side of the Report Builder screen displays the contents of each template report.

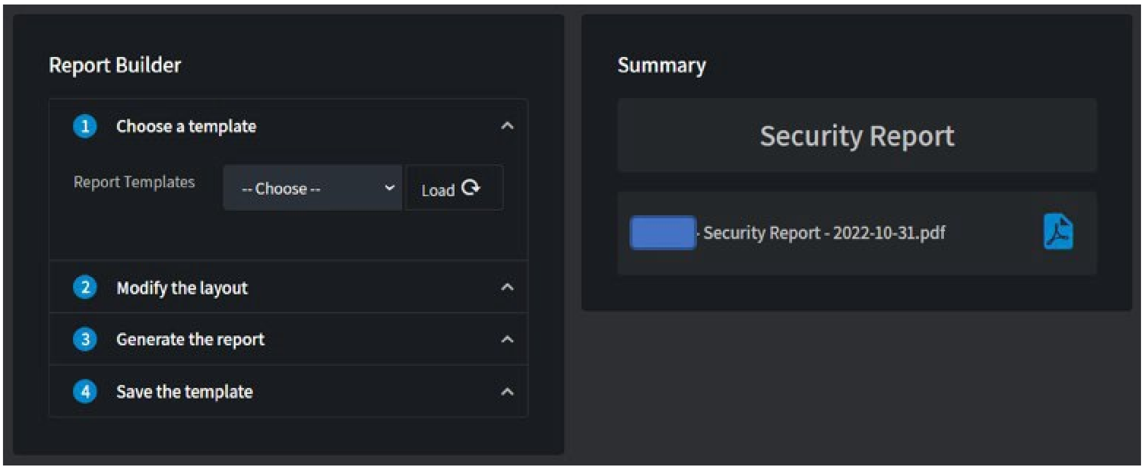


Figure 45: Report Builder Functionality

Step 1: Report Templates

The Report Builder comes with pre-built templates, making common report generation easy and efficient. Using the drop-down box, select the desired report template (see Figure 46 below).

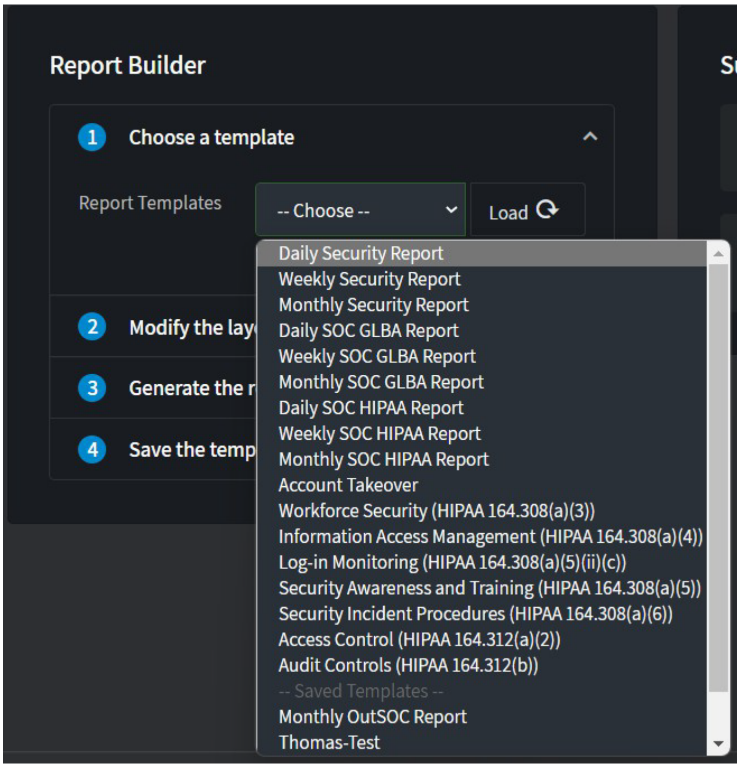


Figure 46: Report Builder Template Options

To view what content is included with a specific report template, select the Load button to refresh the read-only Summary section on the right-side. In the example below (see Figure 47), the Daily Security Report template is selected. When the Load option is selected the read-only Summary section on the right-side refreshed with a list of contents of the Daily Security Report.

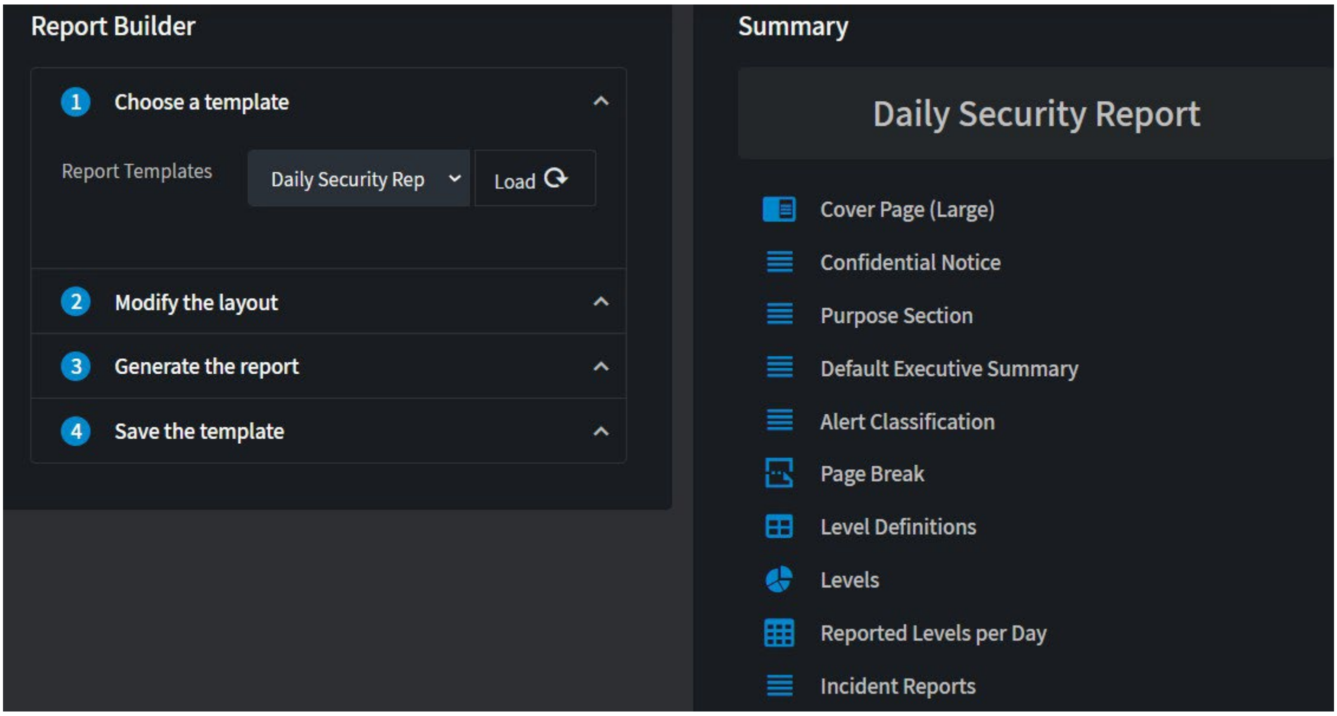


Figure 47: Report Builder with Daily Security Report Template Selected

Step 2: Modify Report (optional)

The second step in the Report Builder allows for modification of a Template. The drop-down boxes can be used to adjust the Report Type, Page Size and Report Title. Major components of the report are listed individually and can be moved using drag-and-drop or removed by selecting the Delete icon (see Figure 48 below).

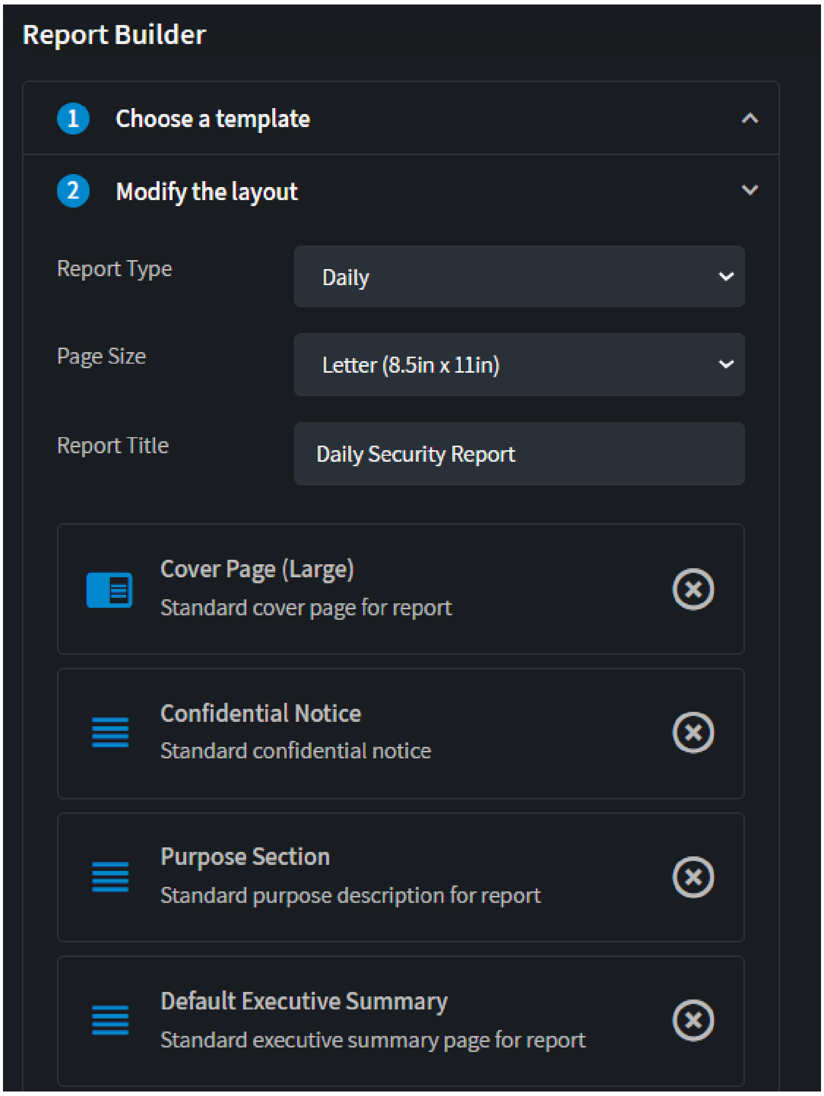


Figure 48: Report Builder Modification Options

Found at the bottom of the Modification options, the Select Component drop-down list provides the option to add new report components. Choose the desired component and select Add (see Figure 49 below). Note: if a component is already included in the report, that option will appear unavailable in the drop-down list.

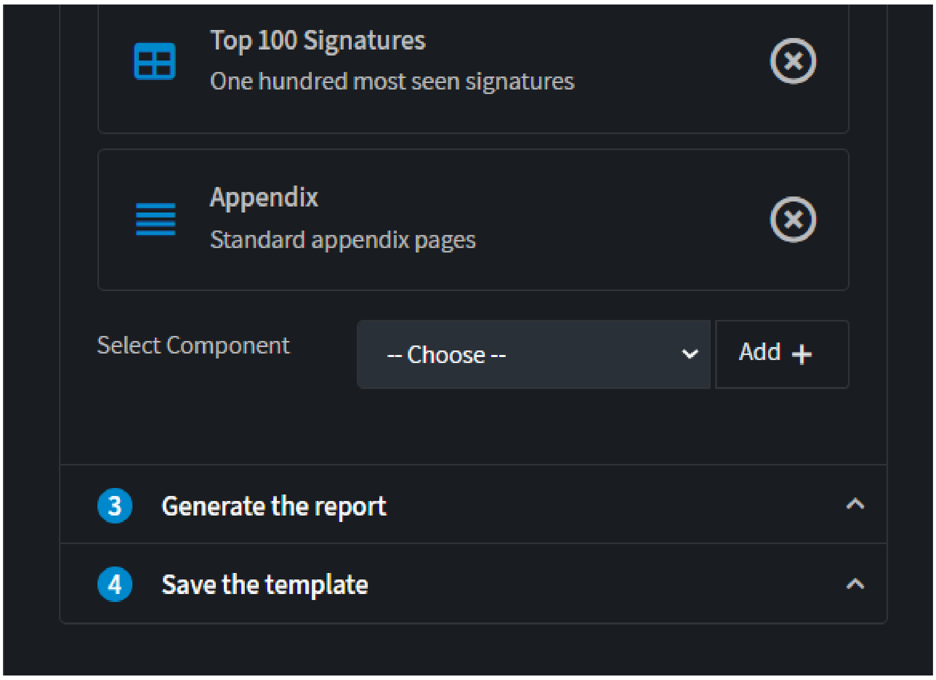


Figure 49: Report Builder Modification Options

Step 3: Generate the Report

Step 3 is final step in choosing report criteria before generating the report. Select the Date Range for the report and edit the File Subject name, if desired. Check the option to save a copy of this report in the File Repository to easily share and retrieve the report. Select Generate when ready (see Figure 50 below).

Note: If creating a report for the current day/month/week/year, be aware that trends and volumes may be truncated/skewed due to incomplete data. To create the most complete reports, a historical viewpoint is recommended.

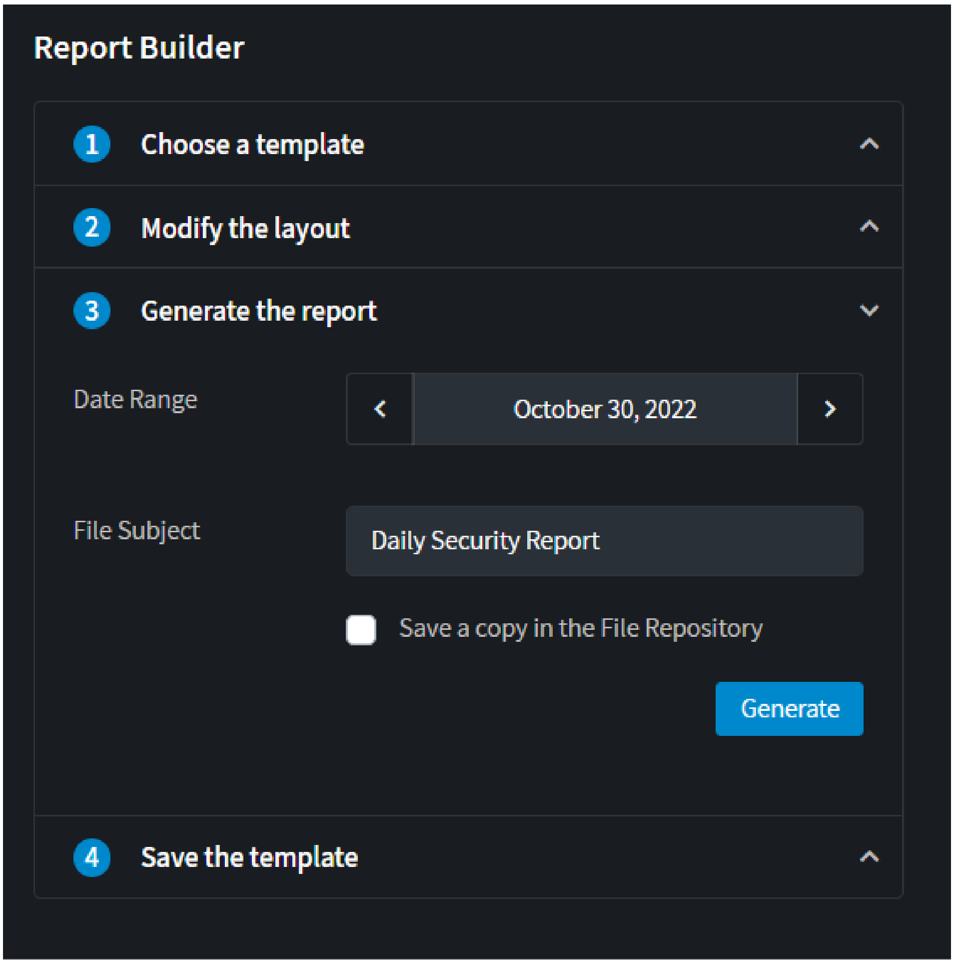


Figure 50: Report Builder > Generate the Report Options

A message box will display, communicating that the report is being generated. Open the PDF prior to selecting the OK button.

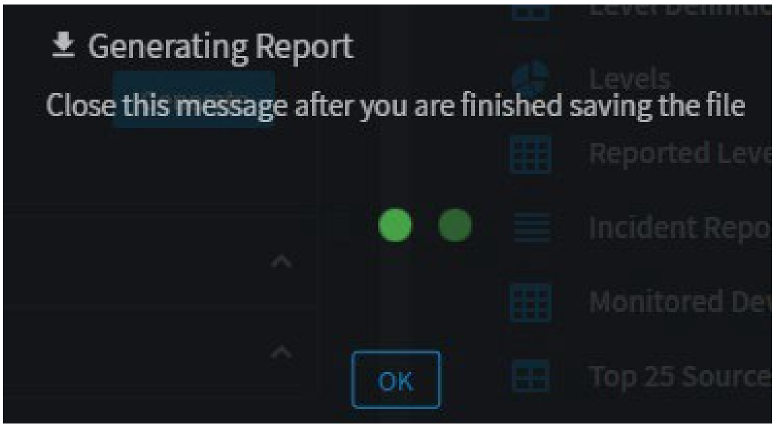


Figure 51: Report Builder Generating Report Message

The new PDF file will be added to the Downloads folder on the browser. Select the file name to open the report.

Figure 52: Report Builder Sample Report

Step 4: Save the Template

To save a customized report as a template, select one of the Save Action options from the drop-down box: Create New Template or Overwrite Existing Template. Enter a Template Name that is specific and unique. Select Save. Now the customized template will appear in the Template drop-down list for future use.

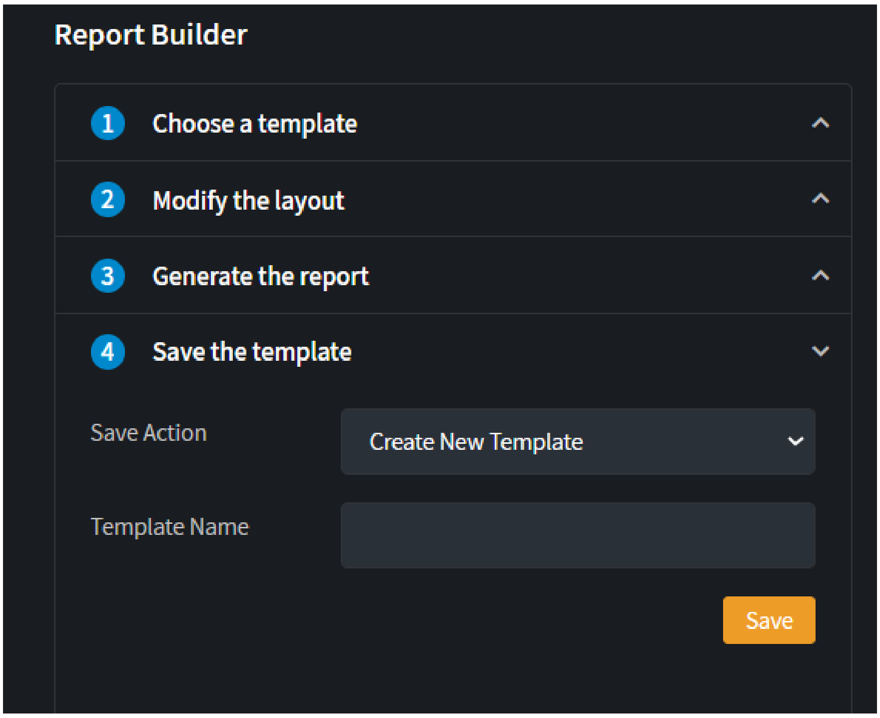


Figure 53: Report Builder Save the Template

Reports > Schedules

The Schedules section of the Report functionality allows a User to schedule reports to be generated on a recurring basis.

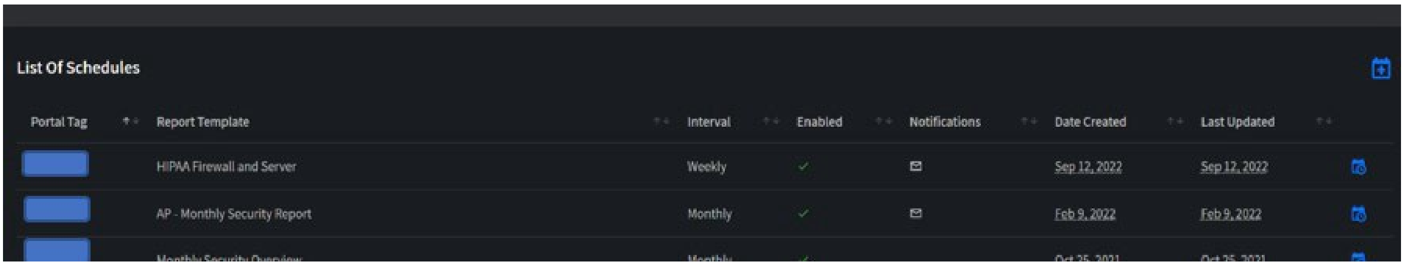


Figure 54: List of Schedules

To add a new scheduled report, choose the Add icon on the right side of the List of Schedules. On the Schedule Report window (see Figure 55 below), choose the Report Template and check Yes to enable this report to be automatically generated. Choose which [Contacts]() should receive notifications when this report is generated. When done, select the Save button.

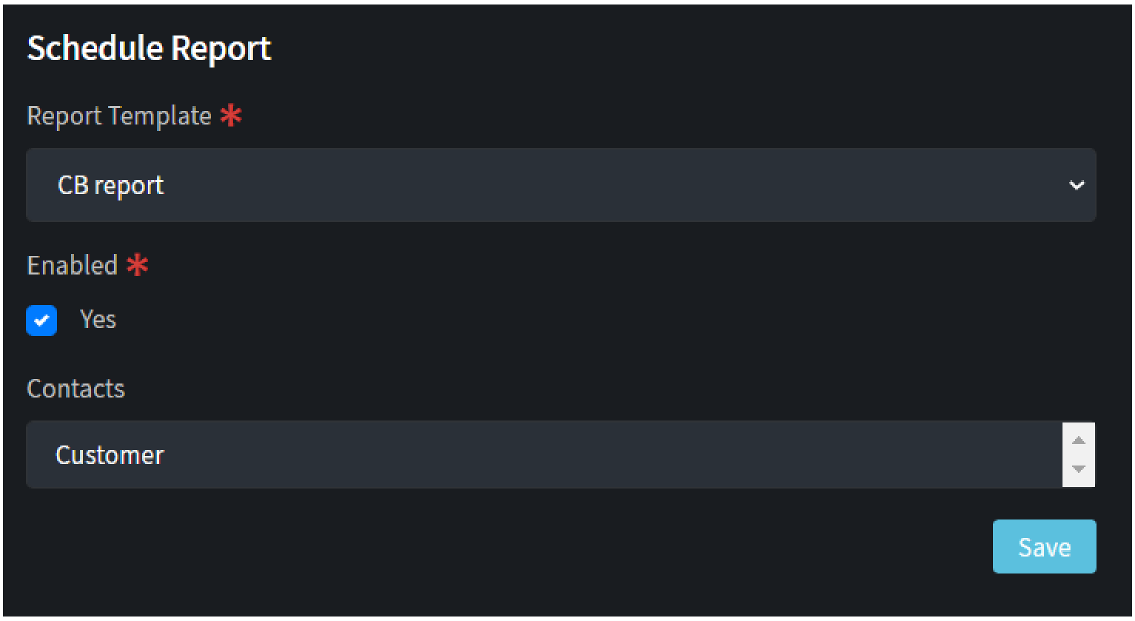


Figure 55: Add Scheduled Report Screen

Recurrence options are defined on each template and include the options of daily, weekly or monthly. Daily reports will run 12 hours after the create date and daily going forward. Weekly reports will run every Sunday at noon. Monthly reports will run on the first day of the next month.

Assets

The Assets feature can be found on the Side Navigation Bar and contains the functionality to manage Assets for the customer account, including Users, Contacts, Devices, Agents, and Groups.

Note: Access to add, edit and delete Asset information is based on User account permissions. If the desired functionality is not available for the User account, create a support ticket to make add/edit/delete requests or to request additional permissions.

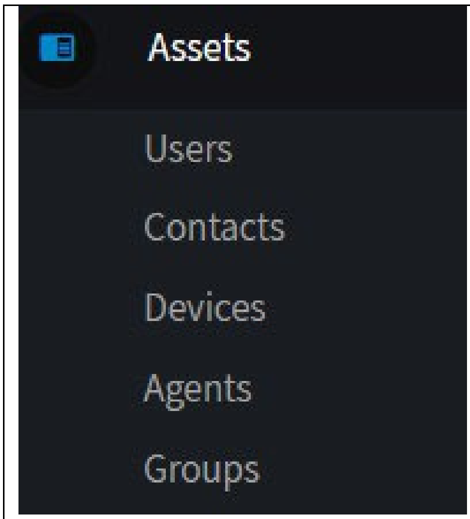


Figure 56: Assets Feature Options

1. **Users** – Individuals authorized to log in to the Lightning Portal.
2. **Contacts** – Points of contact (individuals or group distribution lists) who receive notifications for incidents, support tickets, and reports. Contacts do not need have to a User account (ex: a senior leader may want to receive notifications and reports but has no need to login to the Lightning Portal).

Note: User and Contact accounts are non-syncing. If contact information updates need to be made (ex: email address, phone number), those edits need to be made on both the User account and the Contact.

3. **Devices** – Includes all devices sending logs into the Lightning Portal.
4. **Agents** – Applications installed on endpoints to allow monitoring.
5. **Groups** - Displays groupings of devices (ex: network devices, New York office servers, testing, etc.).

Assets > Users

The User functionality provides the ability to view and manage the Lightning Portal User accounts.

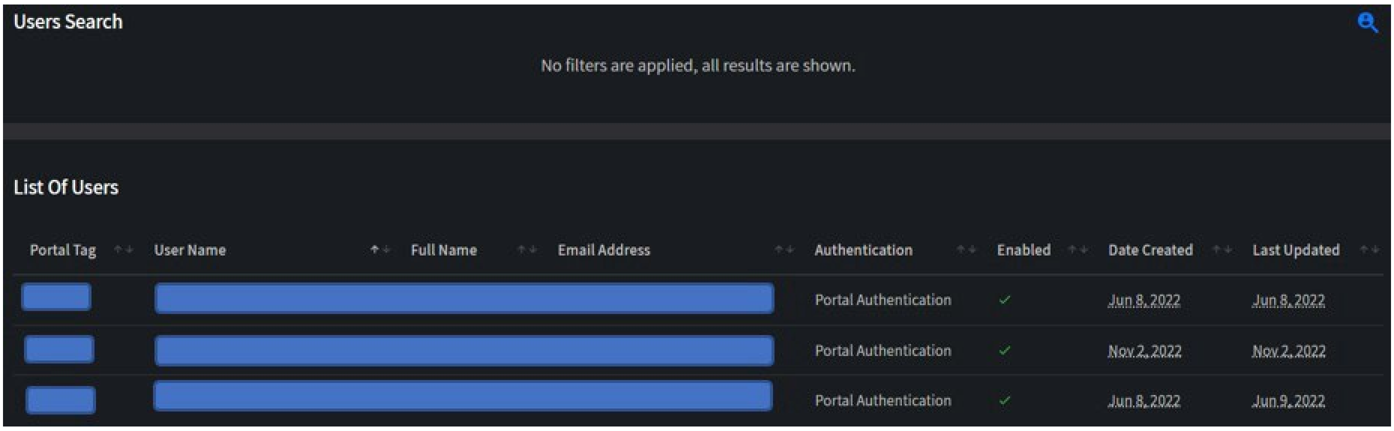


Figure 57: Assets > Users Screen

Users Search

Search for specific User accounts by selecting the Search icon to display the Users Search options (see

Figure 58 below). The data fields for the Users Search feature are listed here:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Username	Enter a partial or full username
Full Name	Enter a partial or full name
Email Address	Enter a partial or full email address
Roles	Use the drop-down list to choose a specific permission-based Role to search
Enabled	Choose the options Yes or No from the drop-down list to search enabled/disabled User accounts

Note: These fields are not required so only enter information in the fields to be searched.

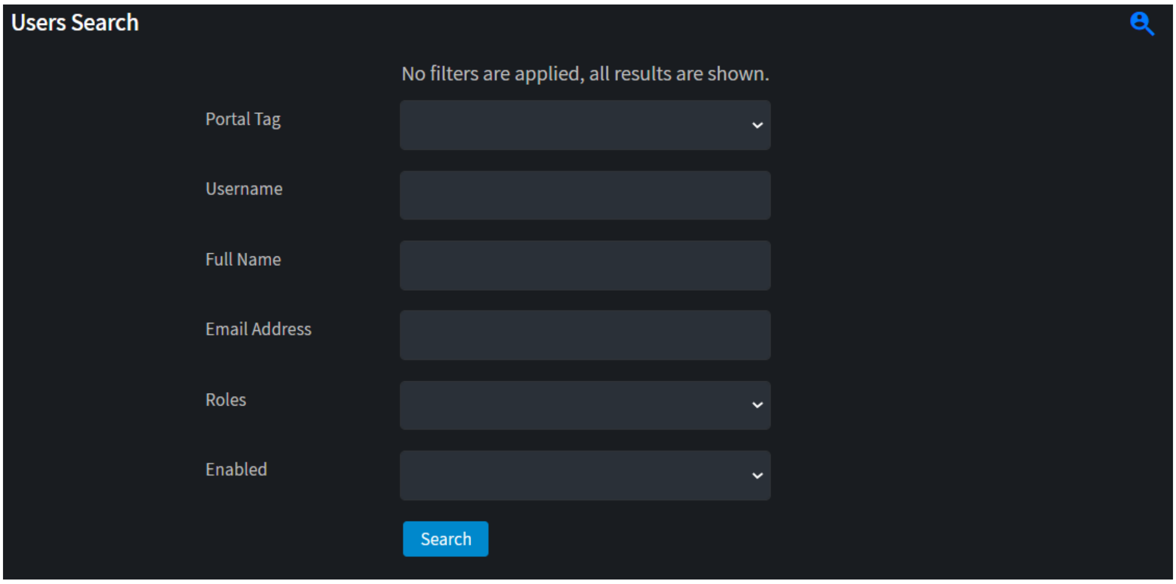


Figure 58: Users Search

Add User

To add a User, select the Add icon on the right-side of the List of Users. Input all required information (marked with red asterisks) and any optional information and then select Save.

Note: If the functionality to Add Users is not available, [create a support ticket]() to request an additional User account.

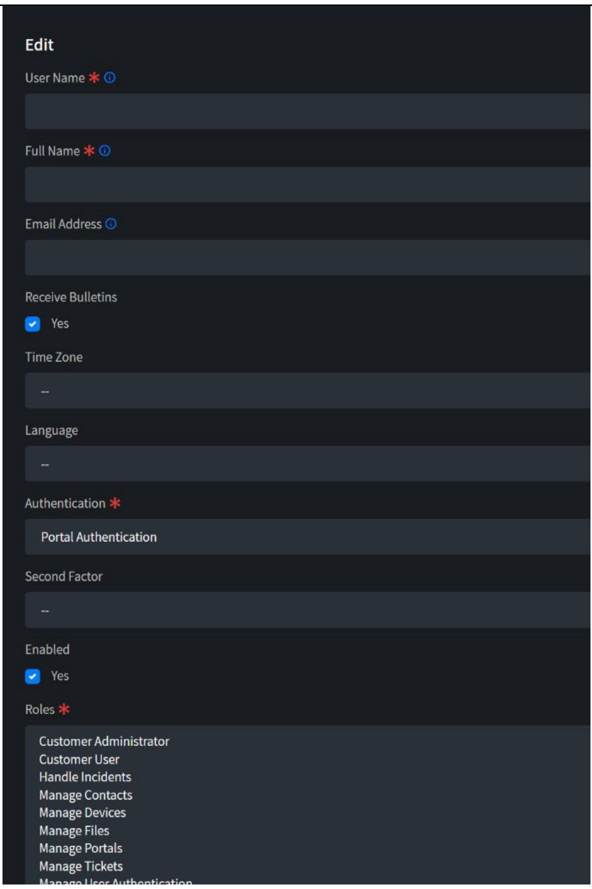


Figure 59: Add User Screen

1. **User Name** – choose a unique username for each User account
2. **Full Name** – input first and last name for the User
3. **Email Address** – input the email address associated with the User account
4. **Receive Bulletins** – check the Yes box for this user account to receive Bulletins
5. **Time Zone** – choose the appropriate time zone
6. **Language** – choose the appropriate language
7. **Authentication** – choose the appropriate authentication option (Portal or Lightweight Directory Access Protocol (LDAP))
8. **Second Factor** – choose the appropriate second factor option
9. **Enabled** – check the Yes box to enable this User account, uncheck the box to disable the account
10. **Roles** – Select a role for this user account, use the CTRL key to select multiple options

Edit User

To edit a User account, first complete a User Search to bring up the desired User account in the List of Users. Select the User Name to open a detailed User Account information window (see Figure 60 below). Select the Edit icon to update the User account information and select Save. Note: If the functionality to edit Users is not available, create a support ticket to request edits.

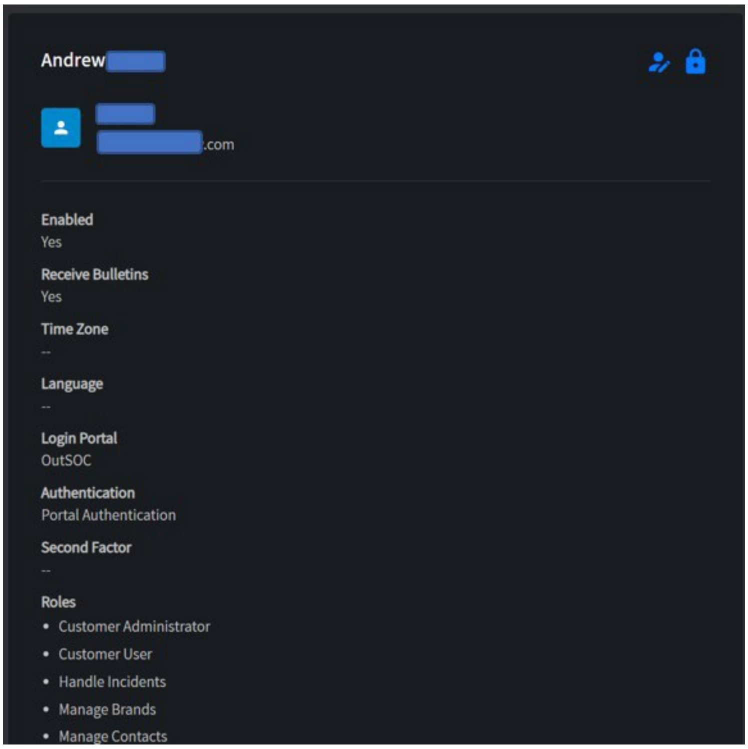


Figure 60: User Account Detailed Information Window

User Password Reset

To set or reset a User account password, select the desired User Name in the List of Users to open a detailed User account information window (see Figure 60 above). Select the Password icon to open the Change Password window (see Figure 61 below).

The system auto-generates an optional suggested password which is compatible with the password restrictions listed. Either enter the suggested password or choose a compatible password and select Save.

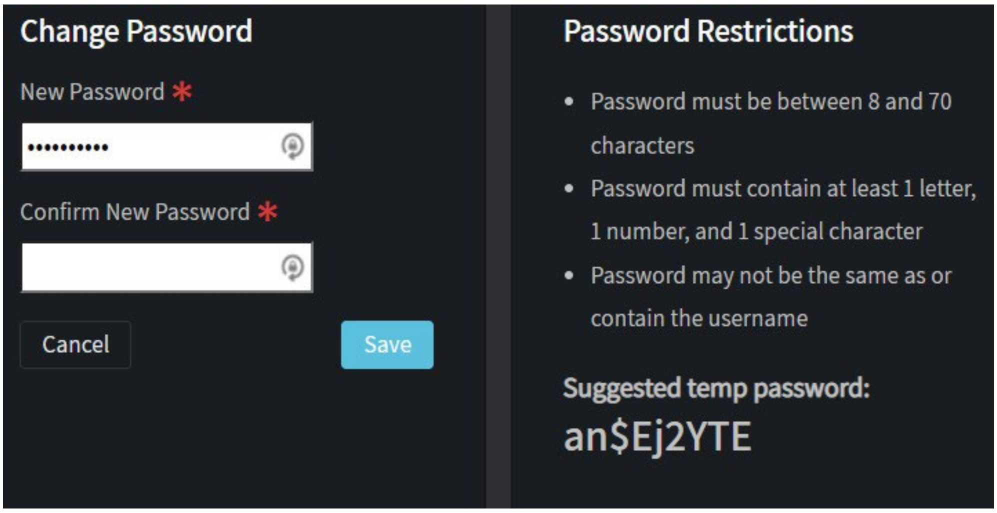


Figure 61: Change Password Window

Disable User

To disable a User Account, select the User Name from the List of Users to open the detailed User account information window (see Figure 60 above). Then select the Edit icon and uncheck the Enabled option and select Save (see Figure 62 below).

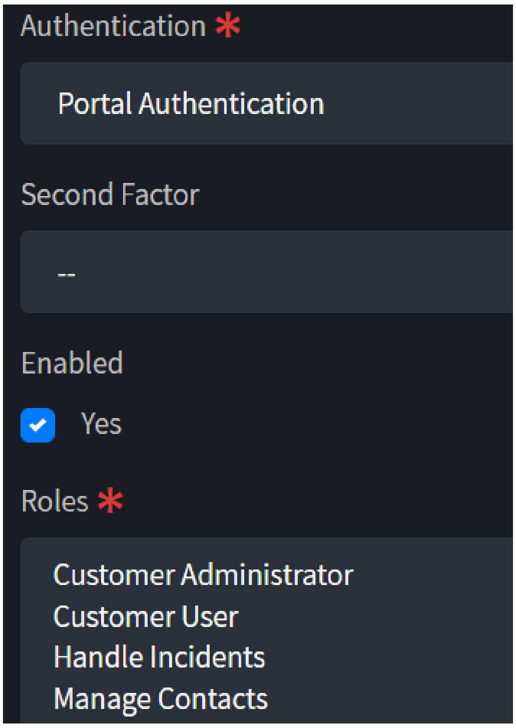


Figure 62: Edit User Window

Assets > Contacts

Contacts are individuals or group distribution lists designated to benotified regarding support and incident tickets (as defined in a Contact Playbook) and/or to receive scheduled reports.

Note: Having a User account does automatically create a Contact account. All Users who want to receive notifications and/or reports should be added as a Contact. Also, any updates to contact information (ex: phone numbers, email addresses) need to be made on both the User and Contact accounts, as the accounts are non-syncing.

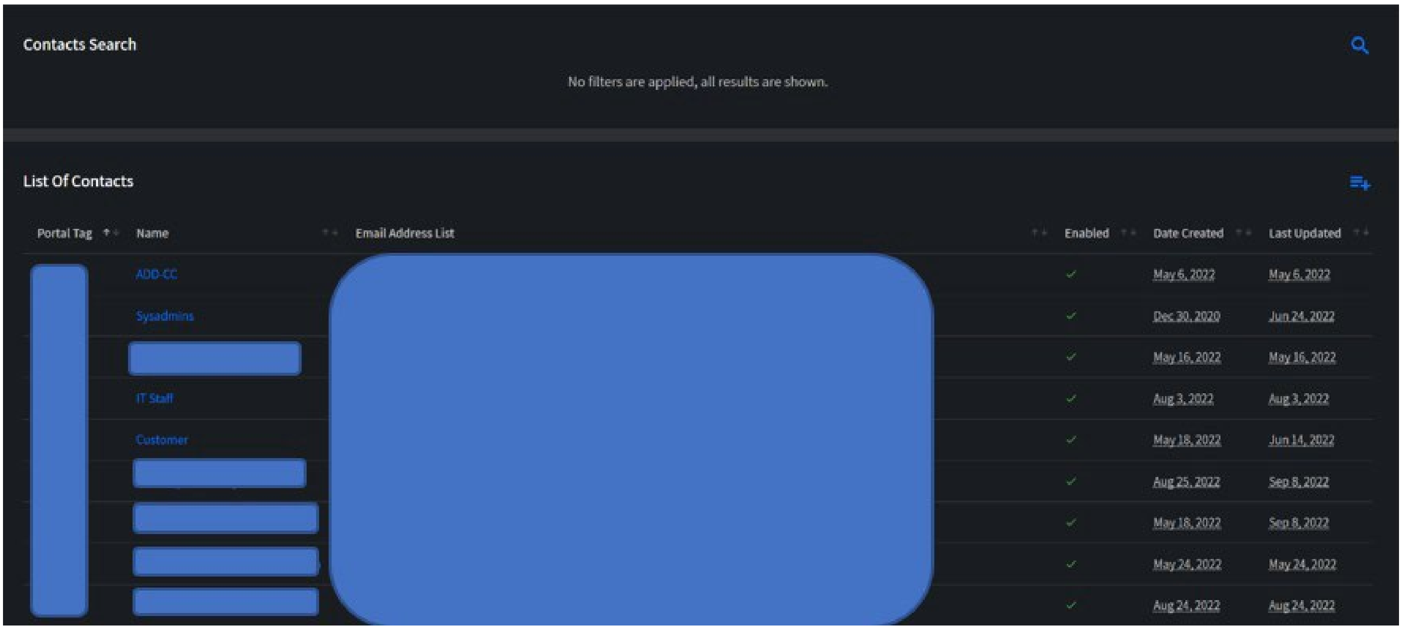


Figure 63: Assets > Contacts Functionality

Contact Search

Search for specific Contacts by selecting the Search icon to display the Contacts Search options. The data fields for the search include:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Name	Enter a partial or full name
Email Address	Enter a partial or full email address
Enabled	Choose the options Yes or No from the drop-down list to search enabled/disabled accounts

Note: These fields are not required so only enter information in the fields to be searched.

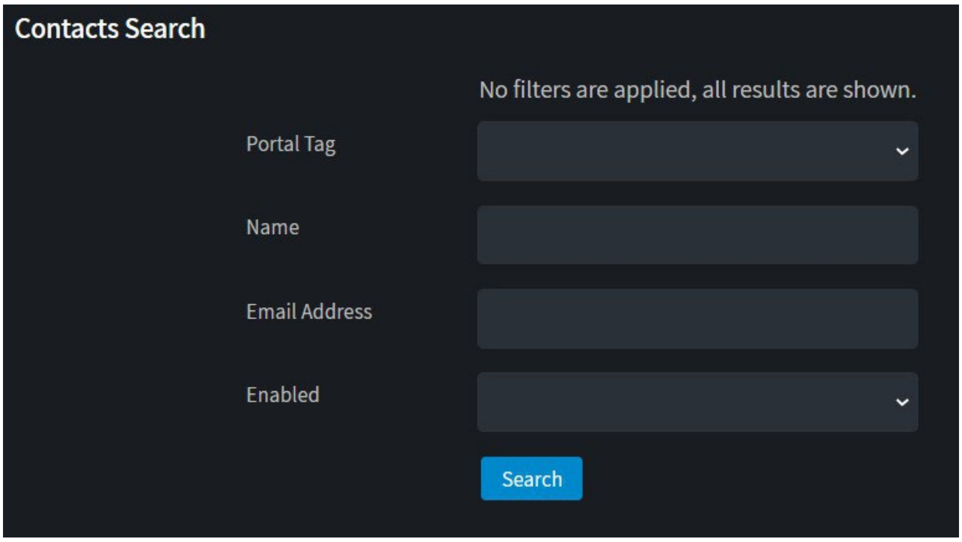


Figure 64: Contact Search Criteria

Add a Contact

To add a Contact, select the Add icon on the right side of the List of Contacts. Input all required information (marked with red asterisks) and any optional information then select Save.

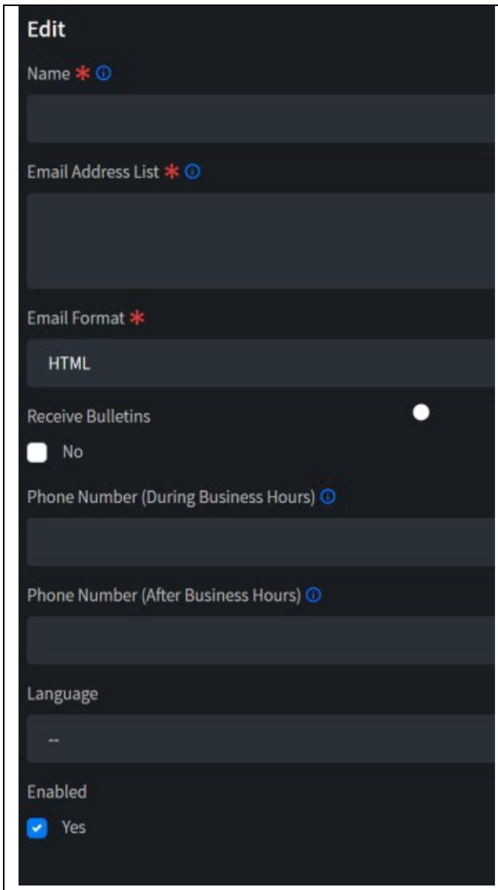


Figure 65: Add a Contact

1. **Name** – input first and last name for an individual or a name for the distribution list

2. **Email Address List** – input the email address(es) to be included on this Contact

3. **Email Format** – choose either HTML or Plain Text

4. **Receive Bulletins** – check the No box for this Contact account to NOT receive Bulletins

5. **Phone Number** (During Business Hours) - enter a phone number for business hours. Note: This information is important because this phone number may be used for Playbook escalations in the case of critical alerts.

6. **Phone Number** (After Business Hours) - enter a phone number that is reliably and consistently answered after hours. Note: This information is important because this number may be used for Playbook escalations in the case of critical alerts.

7. **Language** - choose the appropriate language

8. **Enabled** – check the Yes box to enable this Contact account, uncheck the box to disable the Contact

Edit a Contact

To edit a Contact account, first complete a Contact Search to bring up the desired Contact account in the List of Contacts. Select the Name field to open the detailed Contact account information window (see Figure 66 below). Select the Edit icon to update the Contact account information (see Figure 65 above) and select Save.

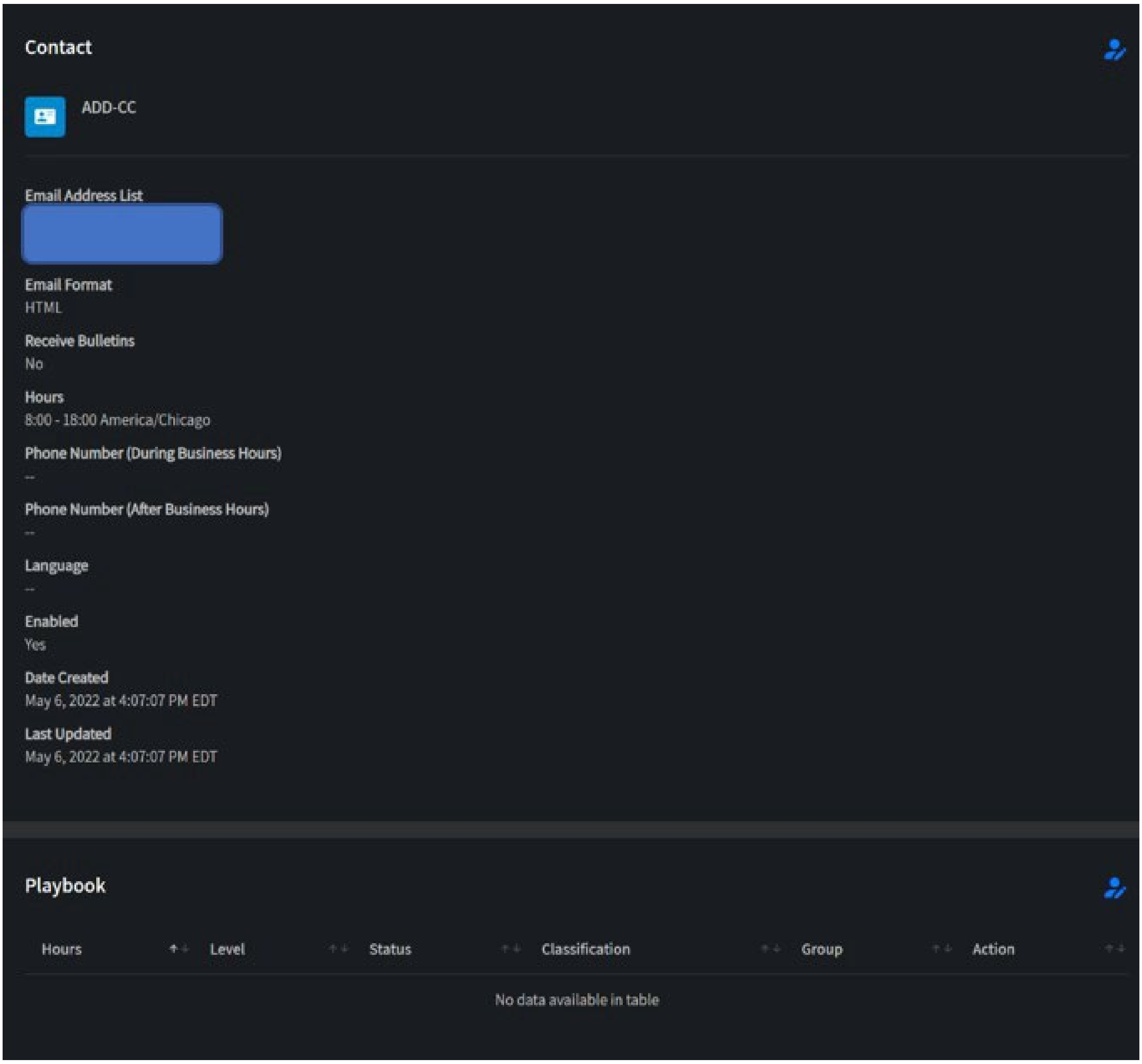


Figure 66: Detailed Contact Account Information Window

Disable a Contact

To disable a Contact, select the Name field from the List of Contacts to open the detailed Contact information window (see Figure 66 above). Then select the Edit icon and uncheck the Enabled option (see Figure 67 below) and select Save. Note: Disabling a Contact will disable associated Playbook(s).

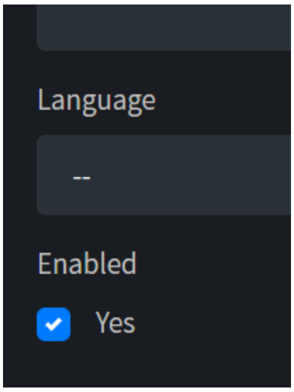


Figure 67: Disable a Contact

Contact > Playbook

The Contact Playbook functionality allows the creation of customized Playbooks to match business needs, available technical resources, and incident response plans. These playbooks define notification preferences based on incident criticality, and multiple Playbooks can be configured to meet notification needs across all scenarios.

Add a Playbook

To add a Playbook, select the Name of the desired Contact to open a detailed Contact information window (see Figure 66 above). Scroll down to Playbook section and select the Add icon .

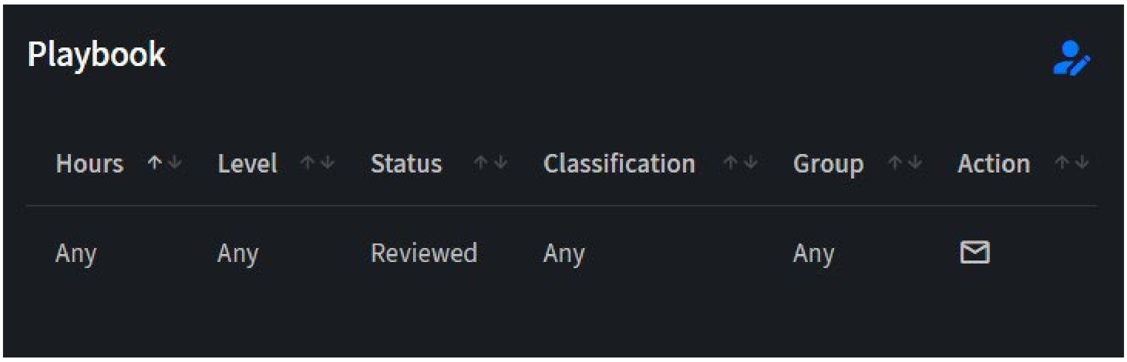


Figure 68: Contact Playbook List

Make selections for the following data fields. Any data field left blank will automatically include all options.

Data Field	Description
Hours	Choose After Business or During Business hours
Level	Choose [Incident](#) level: Info, Low, Medium, High or Critical
Status	Choose Incident status: Active, Reviewed or Closed
Classification	Choose from the list of Incident classifications
Group	Choose the desired [Group](#)
Action	Choose Send Notification or Phone Call

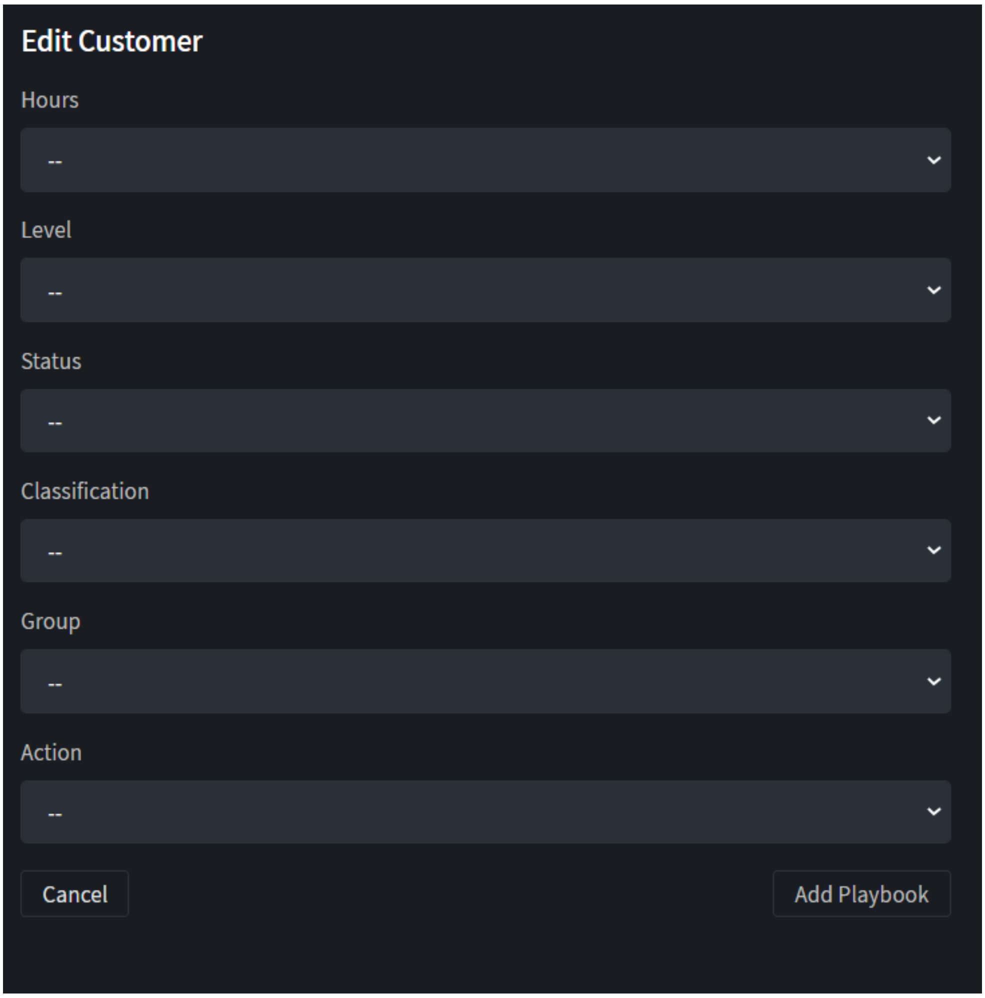


Figure 69: Add Playbook Options

Once a Playbook is created it cannot be edited. If edits need to be made, create a new Playbook and then delete the obsolete version.

Assets > Devices

The Devices feature contains a listing of all Devices that are communicating with and being monitored within the Lightning Portal.

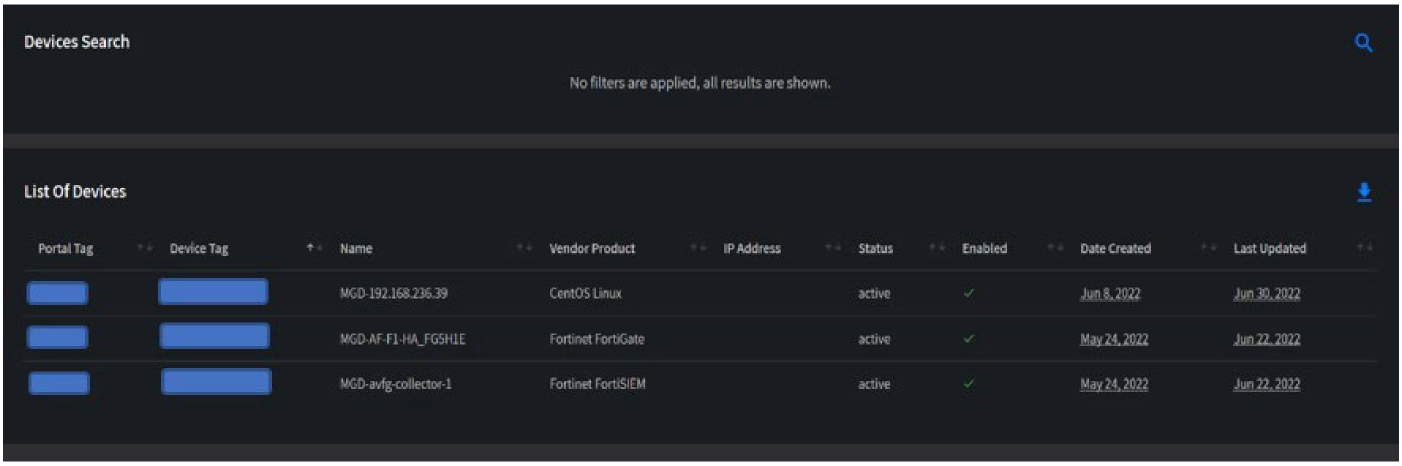


Figure 70: Assets > Device Functionality

Devices Search

Search for specific Devices by selecting the Search icon to display the Device search options (see Figure 71). Search fields include the following:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Device Tag	Enter a full or partial Device Tag
Name	Enter a full or partial Device Name, generally the syslog hostname
Vendor Products	Choose the Device vendor name from the drop-down list
IP Address	Enter a full or partial IP Address
Status	Choose the appropriate Status from the drop-down list, options include: New, Deployment, Tuning, Active, Cancelled
Enabled	Choose either Yes or No from the drop-down list

Note: These fields are not required so only enter information in the fields to be searched.

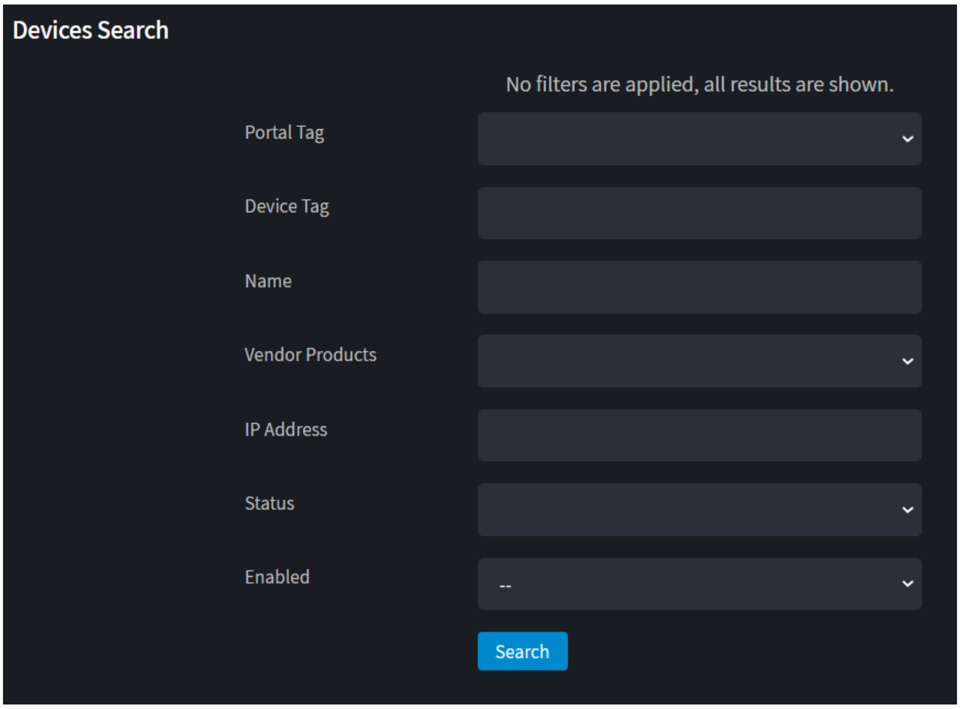


Figure 71: Device Search Criteria

Add a Device

To add a Device, select the Add icon on the right side of the List of Devices. Input all required information (marked with red asterisks) and any optional information.

Note: If a User account does not have the permissions required to add a device, please [create a support ticket] to request a device be added.

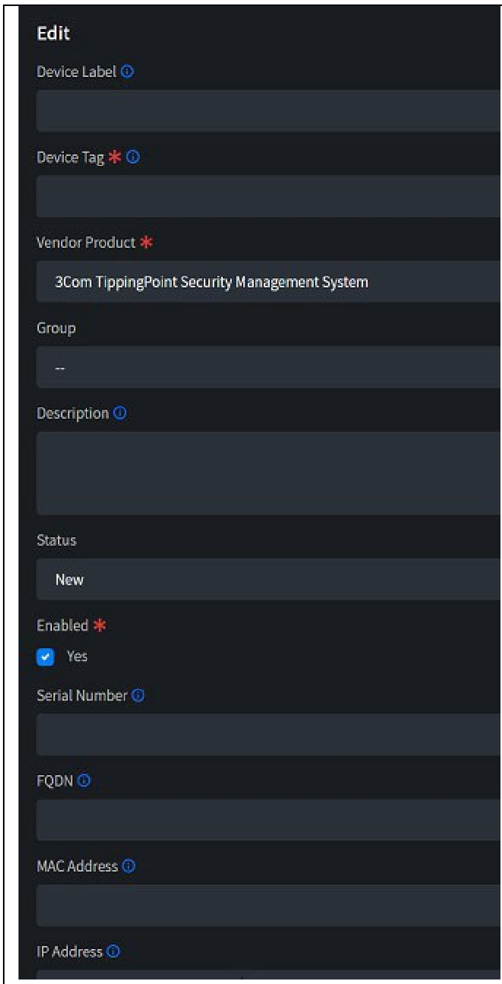


Figure 72: Add Device Criteria

1. Device Label – Enter a descriptive label for the device
2. Device Tag – Enter a device tag by which the device will identified in incoming streams of logs and alerts
3. Vendor Product – Enter the device manufacturer, model, and version
4. Group – Enter the Group to which the device belongs, if applicable (ex: West Region Firewalls)
5. Description – A human readable description of the device, what it is used for, and any additional helpful notes
6. Status – Choose from the options: New, Deployment, Tuning, Active, or Cancelled
7. Enabled – Check the box to enable. Note: disabled devices won't trigger incidents
8. Serial Number – Unique identifier from manufacturer
9. FQDN – Fully Qualified Domain Name
10. MAC Address
11. IP Address
12. NAT (Network Address Translation) IP Address

Edit a Device

To edit a Device, first complete a Device search to bring up the desired Device in the List of Devices. Select the Device Tag to open a detailed Device information window (see Figure 73). Select the Edit icon to update the Device information and select Save.

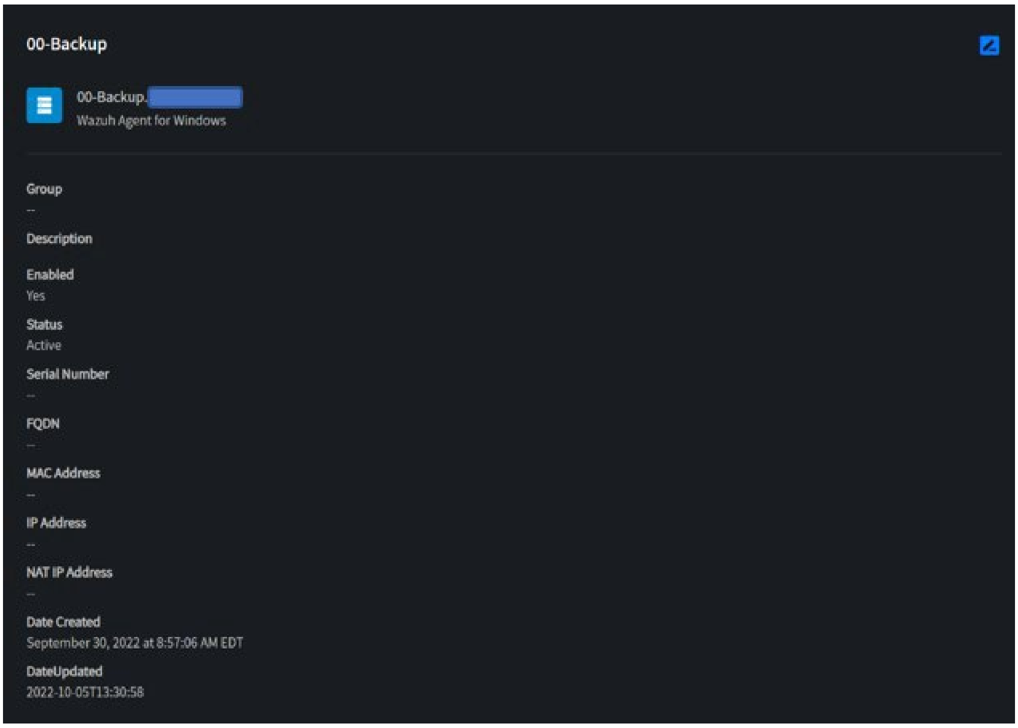


Figure 73: Detailed Device Information Window

Import Devices

The Import Devices functionality allows for multiple devices to be imported at one time via a CSV file. Select on the Import icon on the right side of the List of Devices. The requirements for the imported file are listed on the Import Devices window. Select Browse to locate the desired file, then select Verify.

Note: if the functionality to import devices is not available, [create a support ticket] to import the list of devices.

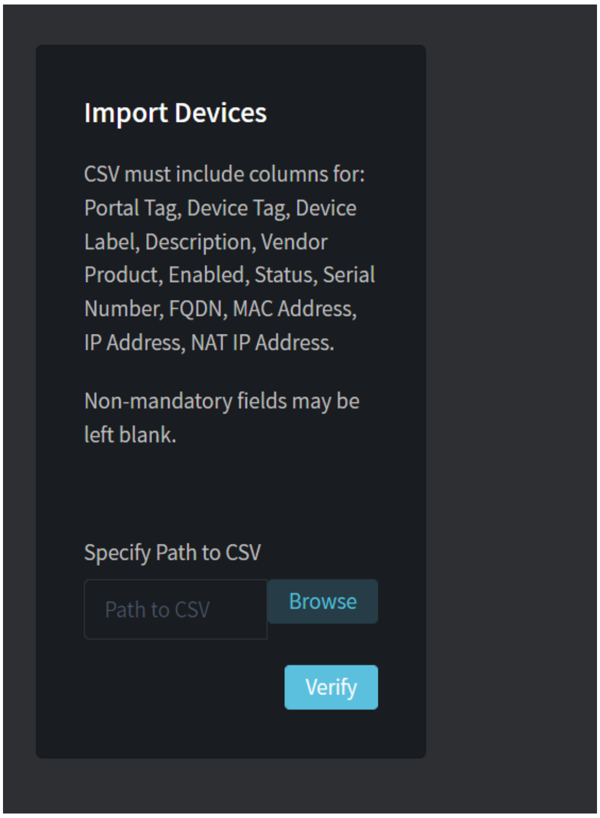


Figure 74: Import Devices Window

Disable a Device

To disable a Device, select the Device Tag field from the List of Devices to open the detailed Device information window (see Figure 73 above). Then select the Edit icon and uncheck the Enabled option and select Save. Note: Disabled devices won't trigger incidents.

Download the List of Devices

To download the current List of Devices displayed, select the Download icon and then select Download CSV. A CSV file will be added to the downloads folder on the browser. Select that file to view the downloaded List of Devices.

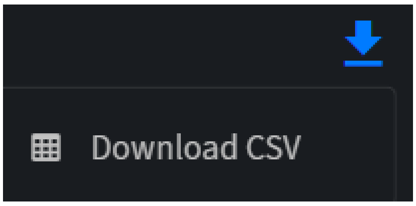


Figure 75: Download List of Devices

Assets > Agents

The Agent functionality in the Lightning Portal contains a listing of all agents forwarding security logs to the portal. An Agent is a deployed piece of software in a customer environment which collects logs and forwards them to the Lightning Portal. Agents may carry out additional response actions as well.

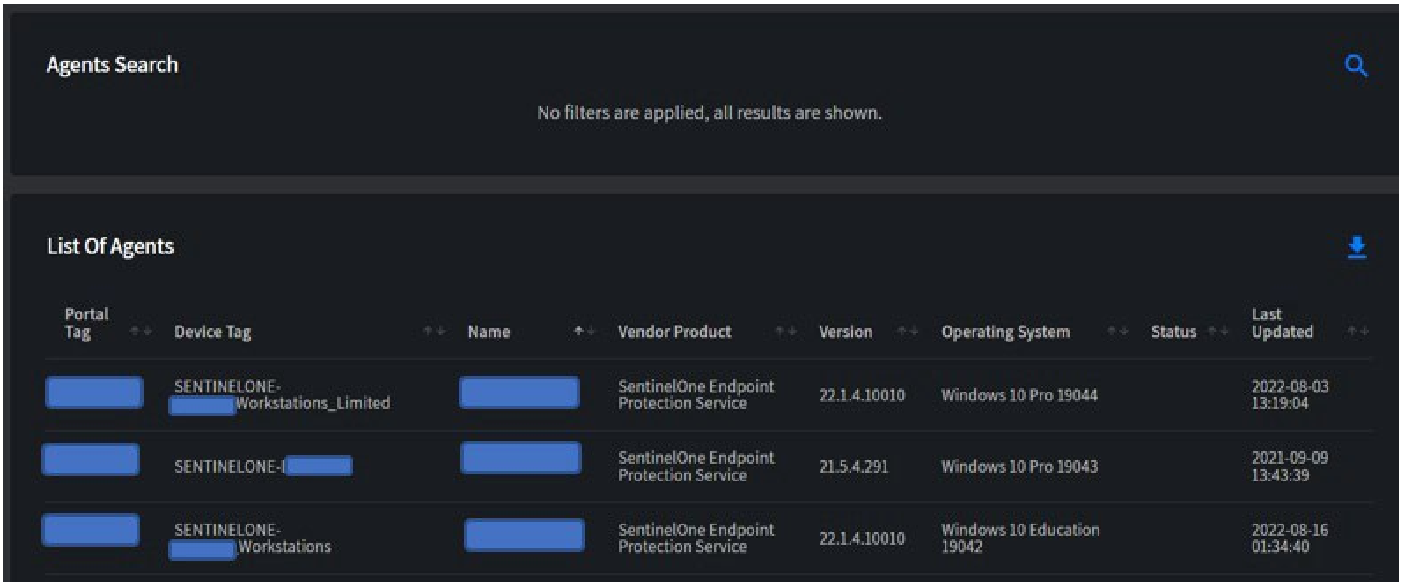


Figure 76: Assets > Agents Feature

Agents Search

Search for specific Agents by selecting the Search icon to display the Agent Search criteria (see Figure 77 below). Search fields include the following:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Device Tag	Enter a full or partial Device Tag
Name	Enter a full or partial Agent Name
Vendor Products	Choose the Agent vendor name from the drop-down list

Note: These fields are not required so only enter information in the fields to be searched.

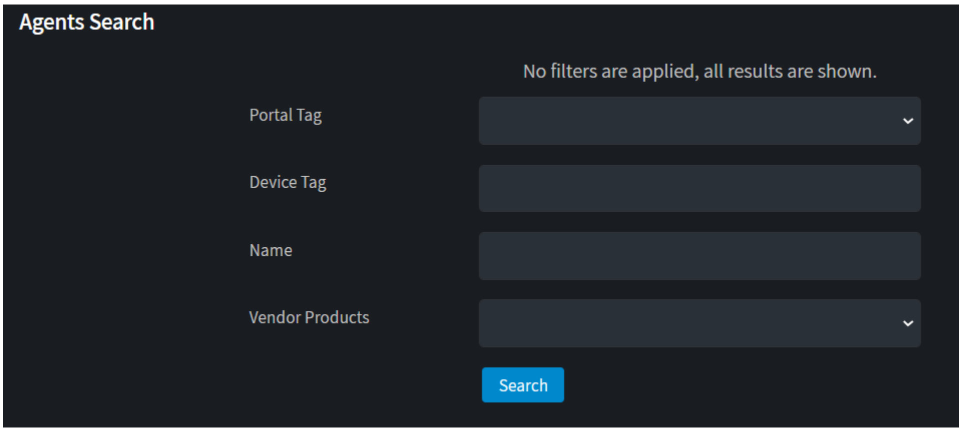


Figure 77: Agents Search Criteria

Assets > Groups

The Group feature in the Lightning Portal displays groups and associations. Groups can be used for logical collection of similar assets (ex: New York office firewalls, Staff EDR agents, etc.)

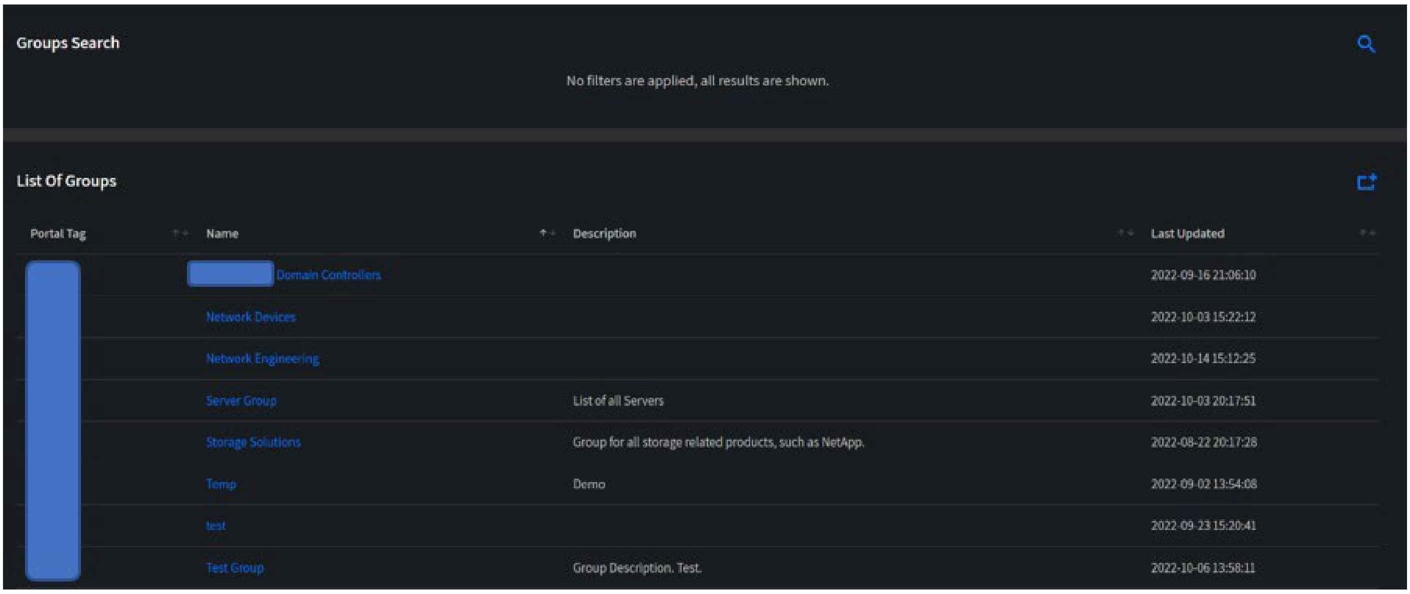


Figure 78: Assets > Groups Functionality

Groups Search

Search for specific Groups by selecting the Search icon to display the Groups Search options. Search field options include:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Name	Enter a full or partial Group Name

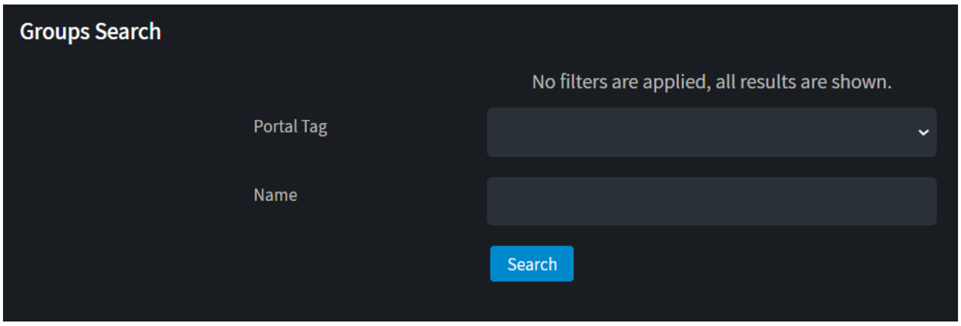


Figure 79: Groups Search Criteria

Add Group

To add a new Group, select the Add icon and enter the Name and Description for the Group. Devices can be added to the group using the Edit Device window. If a User account does not have the necessary permissions to add a Group, create a support ticket to make that request.

Operations

The Operations feature can be found on the Side Navigation Bar and contains functionality to view Response Plans and Bulletins.

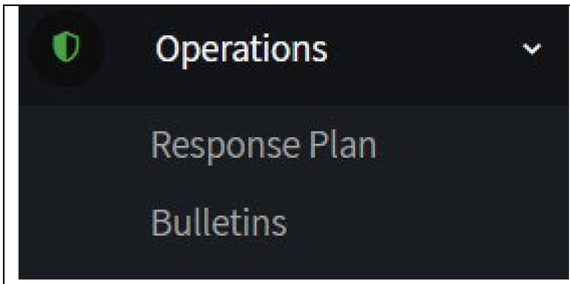


Figure 80: Side Navigation Bar > Operations Menu

1. **Response Plan** - a read-only version of a Playbook
2. **Bulletins** – includes notifications about critical security threats, vulnerabilities, or any significant cybersecurity events.

Operations > Response Plan

The Response Plan is a read-only summary of the Playbook that shows the devices/SIEMs being monitored as well as the contact information for notifications, business hours/after business hours Playbooks, phone support telephone numbers and response times according to the contracted SLAs.

Response Plan

Monitored Devices

OutSOC Tier 2 is actively monitoring the following devices:

Device Tag	Name	Vendor Product	Group
[redacted]	[redacted]	CentOS Linux	
[redacted]	[redacted]	Fortinet FortiGate	
[redacted]	[redacted]	Fortinet FortiSIEM	

Notifications

Email notifications may be sent to the following contacts from notifier@outsoc.com:

Customer

[redacted]

During Business Hours

The following playbooks are executed Monday through Friday from 8:00 - 18:00 America/New_York when ticket criteria are met:

Level	Status	Classification	Action	Contact
Info	Reviewed	Any	Send Notification	Customer

After Business Hours

The following playbooks are executed outside business hours and during weekends when ticket criteria are met:

Level	Status	Classification	Action	Contact
Info	Reviewed	Any	Send Notification	Customer

Phone Support

To call with any questions or escalations:

(800) [redacted]

Response Times

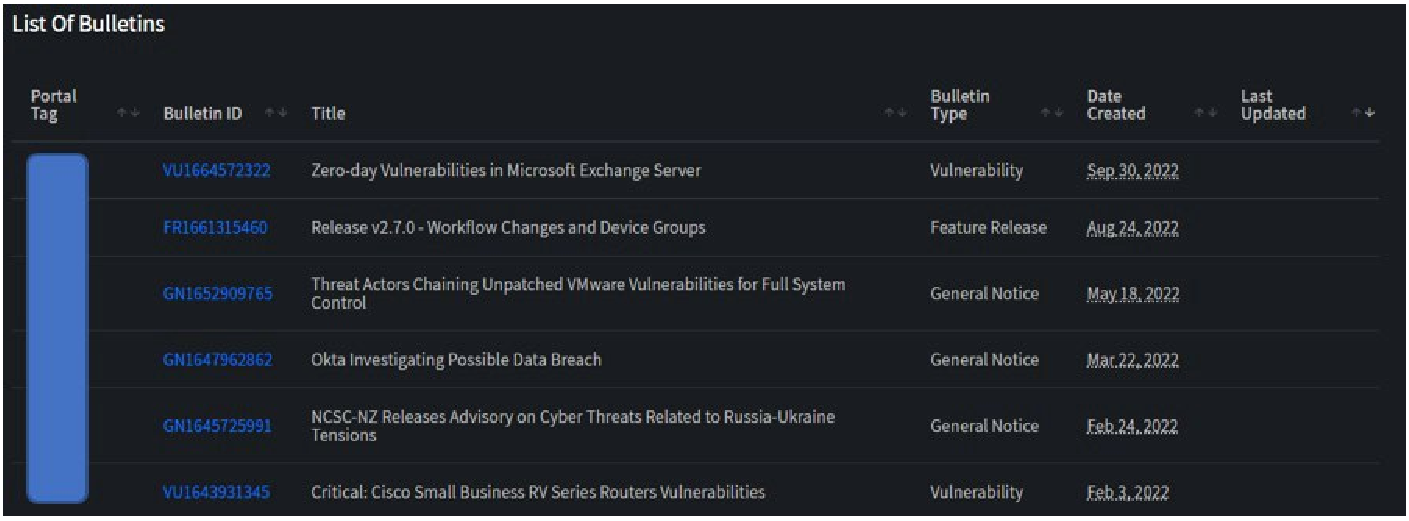
Analysts will handle incidents within the specified times:

1 Low 1d	2 Medium 1d	3 High 10min	4 Critical 10min

Figure 81: Operations > Response Plan

Operations > Bulletins

Bulletins notify customers about critical security threats, vulnerabilities, or any significant cybersecurity events. Select the Bulletin ID to view more detailed information.



List Of Bulletins

Portal Tag	Bulletin ID	Title	Bulletin Type	Date Created	Last Updated
	VU1664572322	Zero-day Vulnerabilities in Microsoft Exchange Server	Vulnerability	Sep 30, 2022	
	FR1661315460	Release v2.7.0 - Workflow Changes and Device Groups	Feature Release	Aug 24, 2022	
	GN1652909765	Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control	General Notice	May 18, 2022	
	GN1647962862	Okta Investigating Possible Data Breach	General Notice	Mar 22, 2022	
	GN1645725991	NCSC-NZ Releases Advisory on Cyber Threats Related to Russia-Ukraine Tensions	General Notice	Feb 24, 2022	
	VU1643931345	Critical: Cisco Small Business RV Series Routers Vulnerabilities	Vulnerability	Feb 3, 2022	

Figure 82: List of Bulletins

Management

The Management functionality includes the ability to view Notifications, Audits, and Sessions to track User activity inside the Lightning Portal.

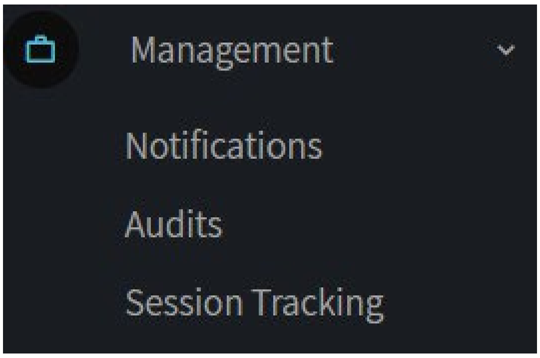


Figure 83: Management Menu Options

Management > Notifications

The Notifications functionality allows users to view and search for Notifications sent via the Lightning Portal.

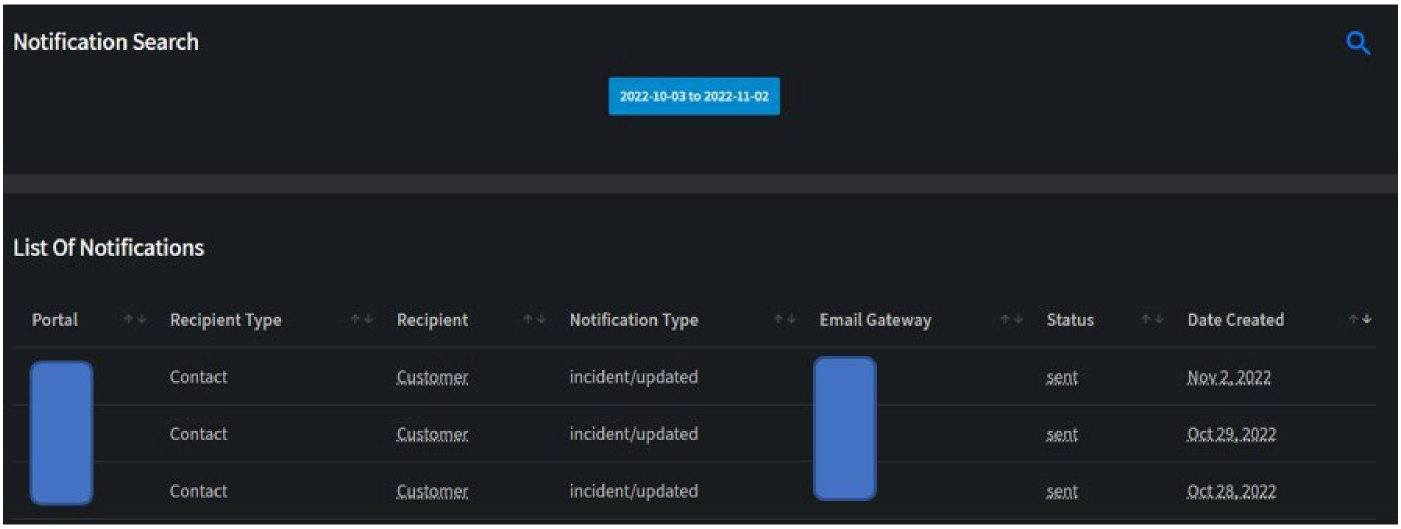


Figure 84: Management: Notifications

Notifications Search

To search Notifications, select the Search icon . The fields available to search include:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Date Range	Choose the date range to search
Search Email Address	Input an email address
Status	Choose Sent or Attempted
Limit	Choose the max number of records to be displayed in the search results

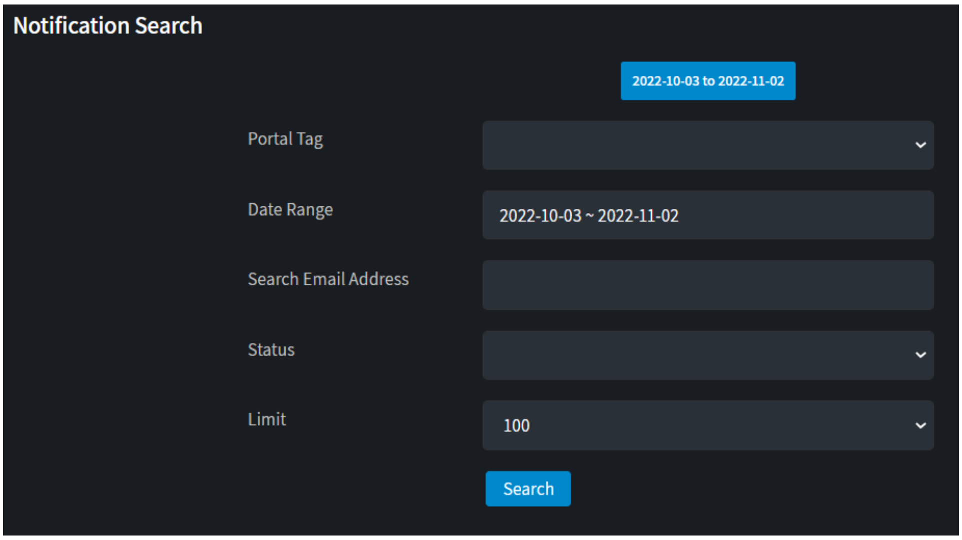


Figure 85: Notifications Search

Management > Audits

The Audit functionality includes a list of all actions taken by Users in the portal.

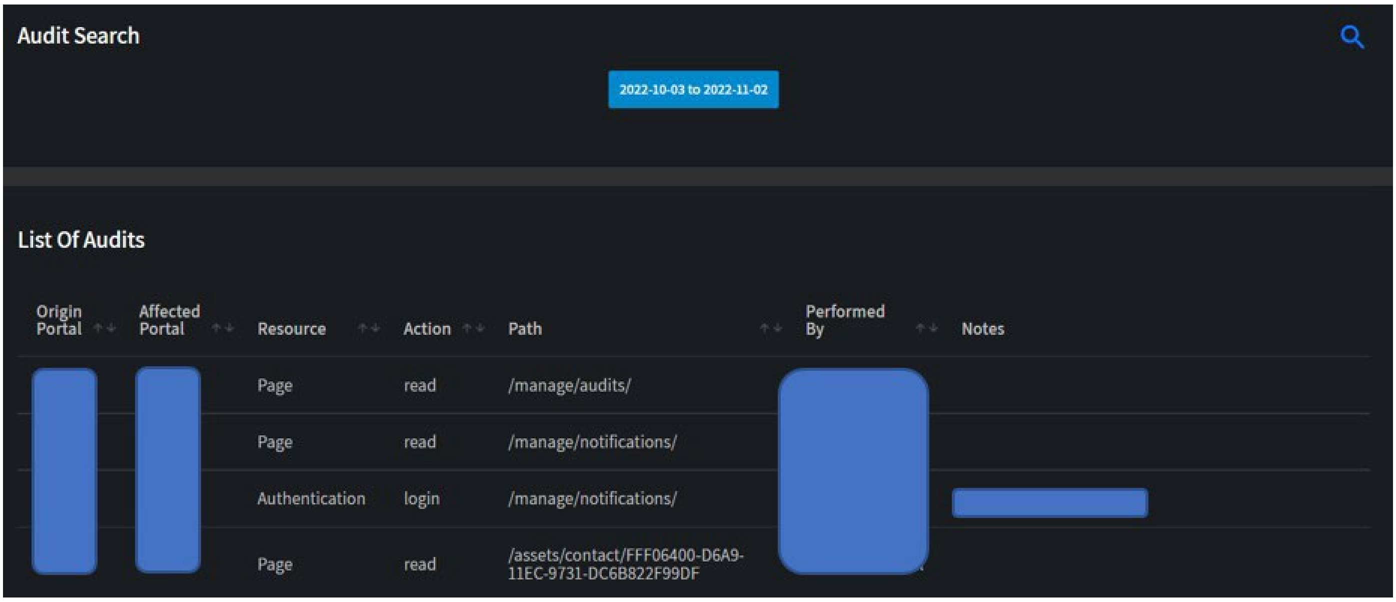


Figure 86: Audits

Audit Search

Utilize the button to open the Audit Search options. Fields to search include:

Data Field	Description
Portal Tag	Select the appropriate Portal Tag from the drop-down list
Date Range	Select the Date range for the inquiry
Resource	Select the Resource from the options (see Figure 88 below)
Action	Select an action from Create, Read, Update, Delete, Login, Logout, Reset
Performed By	Select a User account
Search	Input any desired key words

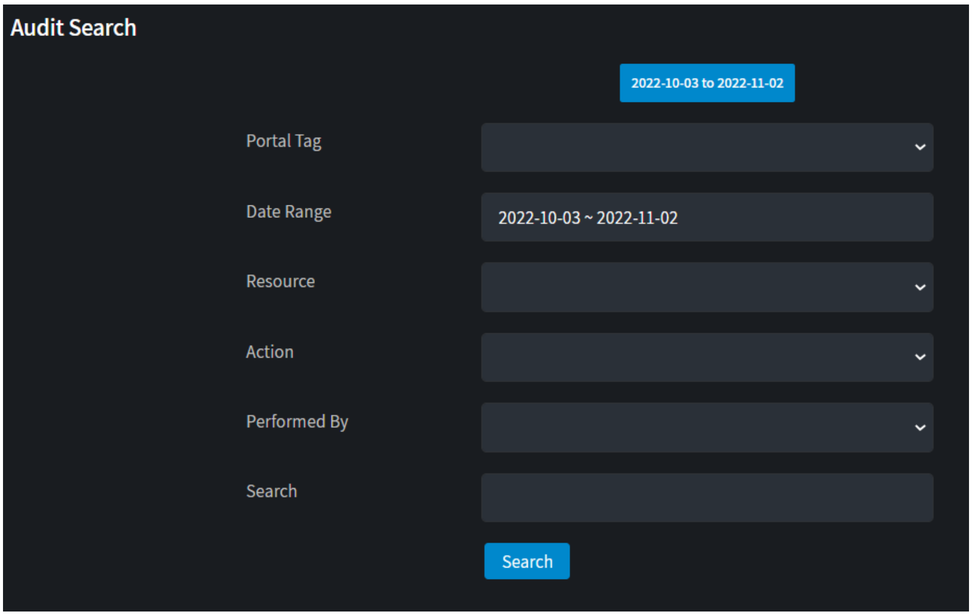


Figure 87: Audit Search

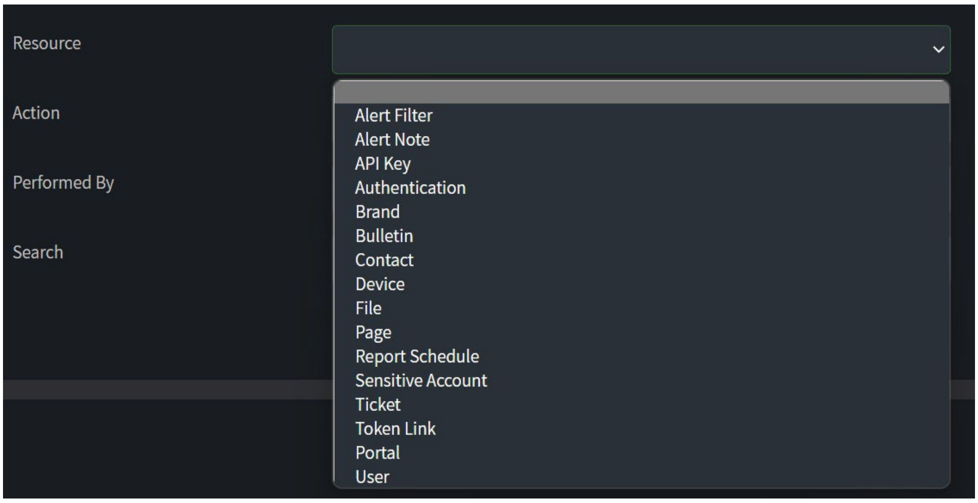


Figure 88: Audit Search: Resource

Management > Session Tracking

The Session Tracking functionality provides visibility regarding Users who have recently logged into the portal.

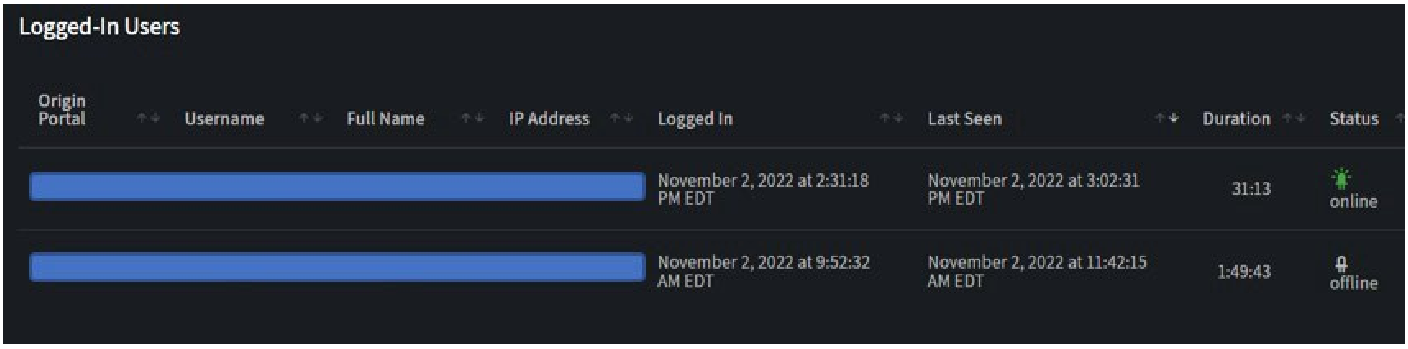


Figure 89. Management Session Tracking

Resources

The Resources functionality provides access to files available for download.

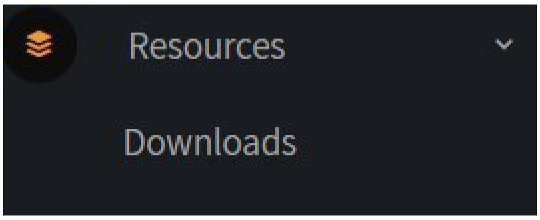


Figure 90: Resources > Downloads

Figure 91: Downloads Screen

If the error message shown in Figure 92 below is displayed, [create a support ticket].

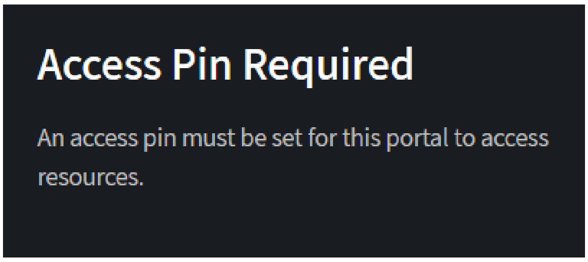


Figure 92: Access Pin Required Message

Glossary

This glossary defines these terms as how they are used in the Lightning Portal and in this document.

Alerts

Lightning Portal alerts are created by ingesting and parsing SIEM, device, and/or system alerts. One Lightning Portal alert may represent a single ingested alert or the Lightning Portal may split bundled events into different alerts, depending upon the pattern and the best method for grouping. Note: Alerts in the Lightning Portal are not atomic representations of SIEM Alerts. An individual Lightning Portal alert may contain all or portions of multiple SIEM alerts.

Bulletin

Bulletins are notifications about critical security threats, vulnerabilities, or any significant cybersecurity events.

Contacts
Contacts are individuals or group distribution lists designated to be notified regarding support and incident tickets and/or to receive scheduled reports. Contact playbooks define how, when and who is notified in specific scenarios.

Device
A device is a source from which log events or alerts are collected. The Lightning Portal does not ingest or process logs from unregistered devices. Note: some SIEM instances may count as one device.

Events
Events are synonymous with log messages or network detections.

Incidents
An incident is a collection of one or more alerts into a single group for analysis. Incidents are the primary unit for SOC security monitoring services to monitor, analyze, and potentially escalate to customers.

- New: A new incident is created when an alert matching a unique pattern is received.
- Existing: An existing Open or Closed incident will be appended if more alerts matching that specific pattern are received, unless that incident is Retired or the alert is filtered.
- Closed: A Closed incident will be activated (reopened) once every UTC calendar day if it is appended to with a new alert.

Notification
An email message created via the Lightning Portal. All notifications can be viewed in the Management > Notifications functionality.

Partner
A partner is a Lightning Portal customer with one or more child customers in the portal level. Partner accounts represent distributors, channel partners, or other hierarchical customer relationships which may have multiple tiers of visibility, escalations, and services for these groupings.

Pattern
An alert pattern is a set of six unique identifying fields of an alert, used to dynamically group alerts into new or existing incidents. Incoming alerts are parsed to extract these fields from the raw alarm or event data. The six pattern fields are:

- Signature
- Device
- Src
- Target (Dst)
- Access
- Action

Playbooks
A playbook is a collection of customer escalation instructions and is defined under a specific contact, The playbook describes who, how and when a customer should be notified of new and updated incidents. Because a playbook is the primary way to stayed informed about security incidents, it is imperative to be thoughtful and thorough when defining a playbook and to keep contact information up-to-date.

Portal

The Lightning Portal user interface is referred to as the portal for customers and the SilverSky support team.

Support Tickets

Support requests are submitted and viewed via the support tickets function. Support Tickets are raised by the customer or SilverSky to initiate a conversation or notify stakeholders about a new support issue or question.

User

A user is an individual with login credentials to access the Lightning Portal.