



# Lightning Customer Portal User Manual for Single Portal User

Version1.3 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

Lightning Customer Portal Introduction
Access and Login
Navigation
Dashboard7
Support Ticket Search
List of Tickets
Create a ticket
Support > Incidents
Incident search21
List of Incidents
Incident Detail View
Incident Notifications27
Support > File Repository
File Uploads
View/Download/Edit/Delete a File
Support > Library
Support > News Feed
Reports
····F
Reports > Report Builder
Reports > Report Builder       33         Step 1: Report Templates       33
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       38
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       38         Reports > Schedules       39
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       38         Reports > Schedules       39         Assets       39
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       38         Reports > Schedules       39         Assets       39         Assets > Users       40
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       38         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       36         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40         Add User       41
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       38         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40         Add User       41         Edit User       42
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       36         Step 4: Save the Template       38         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40         Add User       41         Edit User       42         User Password Reset       43
Reports > Report Builder       33         Step 1: Report Templates       32         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       36         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40         Add User       41         Edit User       42         User Password Reset       43         Disable User       43
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       36         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40         Add User       41         Edit User       42         User Password Reset       43         Disable User       43
Reports > Report Builder       33         Step 1: Report Templates       33         Step 2: Modify Report (optional)       34         Step 3: Generate the Report       36         Step 4: Save the Template       36         Reports > Schedules       39         Assets       39         Assets > Users       40         Users Search       40         Add User       41         Edit User       42         User Password Reset       43         Disable User       43         Assets > Contacts       44         Contact Search       45

## SILVERSKY.

Edit a Contact	5
Disable a Contact	7
Contact > Playbook	3
Add a Playbook48	8
Assets > Devices	9
Devices Search	Э
Add a Device	D
Edit a Device	1
Import Devices	2
Disable a Device	3
Download the List of Devices	3
Assets > Agents	3
Agents Search54	4
Assets > Groups	4
Groups Search	5
Add Group55	5
Operations	5
Operations > Response Plan	5
Operations > Bulletins	7
Management	7
Management > Notifications	7
Notifications Search	3
Management > Audits	3
Audit Search	9
Management > Session Tracking	)
Resources	)
Glossary	L



### **Lightning Customer Portal Introduction**

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	Project Coordinator (during onboarding)		
Login support	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 <u>https://platform.ousoc.com</u>. It is recommended to bookmark this webpage in a preferred browser.

u	Login	× +			- 🗆 X
$\leftarrow$ $\rightarrow$	C û	https://platform.outsoc.com	n		🖾 🚊
			Login		
			Logili		
				rorgerpassiona	
				Login	

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 <u>create a support ticket</u> 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.

Reset	
Reset	

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.



### **Top Navigation Bar**

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



### Figure 5: Top Navigation Bar

ţ≡	Menu Icon: Select the menu icon to minimize or expand the Side Navigation Bar.
> Dashboard	<b>Portal Tag &gt; Current View:</b> Displays the Portal Tag (a six character customer account code) and the current view.
62	<b>Bulletins:</b> Select the bulletins icon to quickly access recent security bulletins posted. The number in red indicates the count of bulletins available for quick review.
Languages 副 English Español ① 日本語	<b>Language:</b> 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 <u>create a support ticket</u> to make that request.
Q	<b>Portal Theme:</b> The light bulb icon allows users to toggle between dark and light themes.
•	<b>View Profile/Log Out:</b> 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.





### Dashboard > Threat Map

The Threat Map displays the region of origin associated with security <u>incidents</u> 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).

SIEM: Multiple Deny Action Fre	om Single Source (199.	-	2	Incident ID	L615 Generate PDF
Threat IP T 199 U	hreat Country Inited States of merica	Threat Score 90		Review Status Updated: October PM EDT	<b>/ed</b> 19, 2022 at 8:36:05
Analysis Classification Security/Network				Info	.cO
Summary 2000 deny events from a single sourc Notes Update 10/19/2022	æ.			Author SIEM Ticket Created	DM ERT
Alert was triggered due to multiple o 199. to 199. via port 37	utbound traffic that we have obse 84 .	erved coming from host	q	Ticket Updated October 20, 2022 at 12:10	0:03 PM EDT
Risk mitigated due to traffic has been required.	n denied/blocked/dropped by the	firewall. No further action	on îs	Analyst Controls	
				Assigned To Dublich Incident	Vec

*Figure* 8: *Incident Report* 

### Dashboard > Alerts Widget

The Alerts widget displays a pie chart representation of the current collection of active <u>incidents</u>, 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).



List Of Incident	ts					
Incident ID ↔ ♦	Title	e 4 - 1	Status 🛧 +	Level ↔	Classification	Last Updated     ↑ ↓
1645	SIEM: Threat Indicator by IP Address: Information Technology (10.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	y i	reviewed		Security/Suspicious Activity	Oct 20, 2022
1309			update		Change/UserAccount	<u>Oct 20, 2022</u>
1539			update		Security/Execution	Oct 20, 2022
-1102	SIEM: Suspicious Behavior (152	1	reviewed		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 <u>incidents</u>, 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

MGD-AF-F1-HA_FG5H1E (AF-F1-HA_FG5H1E)       The atta atta atta atta atta atta atta at	e Devices with Active Tickets widget provides a list of <u>devices</u> ached to an active ticket. Click the first, bolded line to open a vailed device information screen (see Figure 13 below). Click the cond line to open the detailed <u>incident</u> report including the listed vice (see Figure 14 below).
---	---



MGD-AF-F1-HA_FG5H1E	2
Fortinet FortiGate	
Group 	
Description	
Enabled Yes	
<b>Status</b> Active	
Serial Number 	
FQDN 	



SIEM: Inbound Cleartext Password Usage Detected (66.	Incident ID -1022
Threat IP     Threat Country     Threat Score       66.     United States of     90       America     90	Updated Status Updated: November 7, 2022 at 1:56:02 PM EST
Analysis	
Classification Security/Network	Info 💷
Summary Detects inbound usage of protocols that use clear text passwords e.g. FTP, Telnet, POP	Author SIEM
Notes Confirmed okay by customer.	Ticket Created June 6, 2022 at 2:35:04 PM EDT
Repeated alert , similar details as below.	Ticket Updated November 9, 2022 at 5:19:03 PM EST
Telnet sessions between the client and the server are mostly not encrypted, anyone with access to TCP/IP packet flow can observe all of the traffic, listen in, and record potentially sensitive information like logics and encrypted of users economic to the Telpet server.	
like logins and passwords of users connecting to the Teinet server.	
We recommend SSH (Secure Shell) as an Alternative to Telnet.	Analyst Controls
	Assigned To



### 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 Incider	its					
Incident ID ↑↓	Title	Status 📲	Level 🛧 🖗	Classification $^{++}$	Last Updated	<b>↑</b> ↓
1125	SIEM: Excessive End User Mail (1	reviewed	2	persistence	Dec 14, 2022	
1124	SIEM: Large Outbound Transfer (	followup	2	availability	Dec 14, 2022	
1093	SIEM: FortiSIEM Collector Down (avfg-collector-1)	reviewed	2	availability	Dec 14, 2022	
1098	SIEM: Large Outbound Transfer (	reviewed	1	exfiltration	Dec 14, 2022	
.080	SIEM: Traffic to FortiGuard Malware IP List (1	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.





### 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.

Ticket Search		٩	Ticket Lookup
	2022-10-11 to 2022-11-10 updated		
			Lookup
List Of Tickets			<b>•</b>
Ticket ID ↑ ↓ Title	e ^	↑↓ Device T	Fag ^ ↓ Last Updated ^ ↓
	No data available in ta	able	

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.



Ticket Search			Q.
	2022-09-20 to 2	2022-10-20 updated	
Portal T	ag	~	
Device 1	Tag	~	
Date Ra	nge 2022-09-20 ~ 202	22-10-20	
Date Tyj	pe 💿 Created 🔍 Upo	dated 🔍 Both	
Status		~	
Search I	Notes		
	Search		

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.

Ticket Search	2022-09-20 to 2022-10-20 created	or_updated	۹	Ticket Lookup Enter Ticket ID Lookup		
List Of Tickets	ļ					•
Ticket ID 🔷 🔶	Title		• • Escalation Type	• • Device Tag	* + Last Updated	
2742	Additions to the SilverSky and portals	closed	question	1991	Oct 19, 2022	
2733		closed			Oct 11, 2022	
2734		closed	question	01	Oct 11, 2022	

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.

Ticket Search	2022-09-20 to 2022-10-20 updated	>		٩	Ticket Lookup Enter Ticket 10 Lookup		
List Of Tickets	Title ++	Status 🐤	Escalation Type	↑ ÷ Device Tag		Last 9 Updated	•
1359	Constant Constant	followup	question			Oct 20, 202	12
1001		response	question			Oct 20, 202	22
1000		response	question			Oct 20, 202	22
1066		open				Oct 20, 202	22

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.



List Of Tickets					~.		
Ticket ID 🐡 👳	Title	Status ↔	Escalation Type	Device Tag		Last Updated	
370		followup	help	thcforti-1		Oct 20, 2022	
1338		response	question			Oct 20, 2022	
1001		closed	question			Oct 20, 2022	
2359	Access Level	followup	question			Oct 20, 2022	
1000		response	question			Oct 20, 2022	

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.			



New Ticket	
Details	Status Updated:
Title ≭ 🛈	Create
Escalation Type	
- *	Assigned
Summary 🛈	Assigned To
	- •
Devices	
 ATO CHARLES-WORK CiscoFireAmp-9999 Collector-1 Cylance-SP1001 Device-Tag-100	Notifications Contacts
igure 24: Create New Ticket Screen	Churik Caurel Carril

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 <a href="mailto:notifier@outsoc.com">notifier@outsoc.com</a>, 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.



[EXTERNAL]	1000] Comment Added: test reque	st
N notifier@outsor	c.com	← ≪ →
Ticket	-1000	
Summary		
A comment The ticket we updated on a	has been added to Ticket 1000. as generated on April 11, 2022 at 11:00:33 AM April 11, 2022 at 11:27:56 AM BST.	I BST and last
Name Status Level	Follow-up Informational	
	Click to View Ticket	
A support informatio	ticket has been updated with importon, please review.	tant

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 <u>Contact</u>. Notification settings are determined by the <u>Playbook</u> setup in the Contacts functionality.



Incident Search		۹	Incident Lookup	ł.
No filters are applied	all results are shown.			
			Lookup	
List Of Incidents				
Incident ID ↑় Title	↑↓ Status ↑↓	Level 🛧 🗸	Classification 🔷 👳	Last Updated ↑↓
SIEM: Zscaler suspicious we 20452 (192.)	b activity reviewed	1	Security/Suspicious Activity	Oct 31, 2022
SIEM: Traffic to FortiGuard M 3219 (10.	lalware IP List closed	1	Security/Network	Oct 31, 2022
SIEM: Windows Group Creat 1309 (dc.ax19paosusers.svc)	ed or Deleted reviewed	0	Change/UserAccount	Oct 31, 2022

Figure 27: Incident Screen

### Incident search

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



Incident Search	1. <b>Portal Tag:</b> Select the Portal Tag to search from the
No filters are applied, all results are shown.	drop-down list.
Portal Tag 🗸 🗸	2. <b>Device Tag:</b> Select a device from the list to view only
Device Tag 🗸 🗸	incidents for a specific device.
Date Range 2022-10-31 ~ 2022-10-31	3. <b>Date Range:</b> Select the date range to search.
Date Type O O O O O O O O O O O O O O O O O O O	4. <b>Date Type:</b> Select the date created, date updated or both to parrow the search
Status 🗸	5 <b>Status:</b> Select the status of incidents to search (Open
Level 0 Informational 4 1 Low 2 Medium 3 High 4 Critical 4	Active, Reviewed, Updated, Customer Response, Analyst Follow Up, Pending, Closed). If left blank, the search will include all status options.
Classification	6. Level: Select the incident level to search (0 -
False Positive 🗸	Informative, 1 - Low, 2 - Medium, 3 – High, 4-Critical).
Threat IP	Note: each incident level has a response time indicated in the Service Level Agreement (SLA).
Search Text 🔍	7. <b>Classification</b> : Type of threat. NIST threat classification
Limit 100 🗸	8. <b>False Positive</b> : Whether the incident has been marked
Search	as a tuning opportunity (noise to filter, or of low security
Figure 28: Incident Search Criteria	value to suppress or modify).
	9. <b>Threat IP</b> : The source address parsed from any threat (ex: attacker IP or scan origin)
	10. Search Text: Use this option to search by keywords.
	11. <b>Limit:</b> 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.
	• <b>Reviewed</b> : 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.
	• <b>Pending</b> : an incident in a paused/holding state.
	• <b>Closed</b> : 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 <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.
	<ul> <li>Medium (2) – May have a <u>medium level of impact</u> on the network or system and could</li> </ul>
	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
	maiware infection, data leakage, and disruption of operations due to network or system
	down time. Examples: download of malicious software, leakage of file from internal
	exploit launching
	• Critical (1) – 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 Incide	ents				
Incident ID ↑↓	Title	Status ↑+	Level 🖘	Classification	Last Updated ↑↓
1819	SIEM: Windows Failed Login Attempt using an Expire Account (	reviewed	0	Security/Authentication	<u>Oct 31,</u> 2022
4568	SIEM: Executable file posting from external source	update	0	Security/Execution	Oct 31, 2022
3621	SIEM: IPS Events	update	2	Availability	<u>Oct 31,</u> 2022
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.



SIEM: Multiple Logon Failures:	VPN (		Incident ID	116
Threat IP	Threat Country United States of America	Threat Score 90	Close Status Updated: Novemb	ed er 4, 2022 at 11:12:03
Analysis Classification Availability			Medium	•0
Summary Detects multiple VPN logon failures Notes Multiple login failure from source IP towards	5 consecutive failures in a 10 minut	e period munications LLC, US, Clean)	Author SIEM Ticket Created October 28, 2022 at 11:02 Ticket Updated	:03 AM EDT
Username: Can it be verified if this traffic is legitir <b>Remediation</b> 	mate		Analyst Controls	
			Assigned To Publish Incident	Adam (

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).



Devices • Event Count 2		۲	Publish Incic False Positiv Suppress Ale Alert Pattern	lent e irts	Yes No No
Recent Alerts Source •• Target •• Signature SIEM_Brute_F	++ Access ++ orce_Host_Login_Success _Logon_Failures_VPN	Last Seen * 2022-10-28 15:03:30 2022-10-28 14:59:00	Handling Ne Entered by PM Firewalls for a SilverSky sect is Managed by send email to	otes Juli device urity engineerii y Silversky. For	<b>un 24, 2022, 2:31:47</b> s are managed by ng team. This client IP blocks, please
Comments		¢	Notification Contacts	s	
			Recipient	Status sent	Date Created

### 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 <u>Contact</u>, if designated as such in the <u>Playbook</u>.

Comments	Ð
Add Comment 🛈	
	4
	Save

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).

-32: NCIDENT SU Detects netwo	19] SIEM: Traffic to IMMARY: ork traffic to FortiGu	FortiGuard Malware	IP()
ECHNICAL [	DETAILS:		
	Threat Name	SIEM: Traffic to Fort	iGuard Malware IP List (10.
WHAT	Level	1	
	Alert Count	14	
WHY	Signature	SIEM_Excessive_End SIEM_Traffic_to_For	I_User_Mail tiGuard_Malware_IP_List
WHEN	Timestamp	Date Created: Last Updated:	August 3, 2022 at 8:25:05 AM EDT October 31, 2022 at 12:03:04 PM EDT
WHERE	Target	Reporting Devices: Target IP:	3,
wно	Threat	Threat IP: Threat Country:	Private IP Address

Figure 35: Sample PDF Incident Report

### **Incident Notifications**

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

Escalation and notification emails will originate from <u>notifier@outsoc.com</u>, 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.

SILVERSKY

Summary	
Incident 589	2 has been updated.
The incident was gen updated on July 1, 20	erated on June 29, 2021 at 3:13:04 PM EDT and last 21 at 11:33:24 AM EDT.
Name	OutSOC
Status	Closed
Level	Medium
Threat Country	Availability
Threat Score	
Total Alerts	1

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.

File Uploads						<b>±</b>
File Listing						۵
File Type **	Portal Tag *	File Name	*↓ t-2022-09.pdf	Folder Saved Reports	File Size ↑↓	Oct 5, 2022
					« Previ	ous 1 Next »

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).

SILVERSKY



### 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).



File Listing					٥
File Type ↔÷	Portal Tag ↑↓ File Name	Folder	File Size ↑↓	Date Created	
	- NSPARC Exec Security Report - 2022-10-30.pdf	Scheduled Reports	118 KB	Oct 31, 2022	
	- Security Report - 2022-10-30.pdf	Scheduled Reports	1.2 KB	Oct 31, 2022	
	Daily Security Report - 2022-10-30.pdf	Scheduled Reports	121 KB	Oct 31, 2022	
	Daily Security Report - 2022-10-30.pdf	Scheduled Reports	94 KB	Oct 31, 2022	

Figure 39: File Listing with Row Selected

### ${\it Right\, click\, anywhere\, on\, the\, row\, and\, select\, an\, option.}$

File Name	<b>↑</b>	File Size ↑↓
- NSPARC Exec Security Report - 2022-10-30.pdf	Scheduled	118 KB
- Security Report - 2022-10-30.pdf	1 Rows Selected	1.2 KB
Daily Security Report - 2022-10-30.pdf	Download	121 KB
Daily Security Report - 2022-10-30.pdf	Delete	94 KB
- YW SOC-SIEM Security Executive Daily Report - 202	2-10- Scheduled	110 KB

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

Edit File	
- Monthly Security Report - 2022-09.pdf	152.6 KB
Туре	
<b>Size</b> 152.6 KB	
Hash 73cdcf3069797144c3c28538721add3719f2ac155186aba96cf14803862e9dc0	
Description 🛈	
Cancel	Save

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.



# Folders

- Library (0)
  - → Information Security Policies (0)
  - → On-Boarding Documents (0)
  - → Sales and Marketing (0)
  - └> User Guides (0)
- → Reports (1)
  - → Saved Reports (0)
  - → Scheduled Reports (0)

### 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 <u>News Feed widget</u> on the Dashboard or from the Side Navigation Bar > Support > News Feed.

RSS Feed	
The White House's global ransomware summit couldn't come at a better time	^
Ordinary web access request or command to malware?	^
Apple patches actively exploited iPhone, iPad kernel vulns	^
Singapore hosts ICS/OT cybersecurity training extravaganza	^
Liz Truss phone hack claim prompts calls for investigation	^
This Windows worm evolved into slinging ransomware. Here's how to detect it	^
The top cloud cyber security threats unpacked	^
Biden now wants to toughen up chemical sector's cybersecurity	^

# 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.



**Reports > Report Builder** 

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.

Report Builder		Summary
1 Choose a template	^	Daily Security Report
Report Templates Daily Security Rep - Load G		Cover Page (Large)
2 Modify the layout	~	Purpose Section
<b>3</b> Generate the report	^	Default Executive Summary
4 Save the template	~	Alert Classification
		Page Break
		🖽 Level Definitions
		😓 Levels
		🗰 Reported Levels per Day
		Incident Reports

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).



Report Builde	r	
1 Choose	a template	^
2 Modify	the layout	~
Report Type	Daily	~
Page Size	Letter (8.5in x 11in)	~
Report Title	Daily Security Report	
Cov Star	<b>rer Page (Large)</b> ndard cover page for report	$\otimes$
E Cor	nfidential Notice ndard confidential notice	$\otimes$
E Pur Star	pose Section ndard purpose description for report	$\otimes$
E Def	ault Executive Summary	$\otimes$

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.



⊞	Top 100 Signatures     Signatures       One hundred most seen signatures     Signatures				
	<b>Appendix</b> Standard app	endix pages		$\otimes$	
Select Co	mponent	Choose	~	Add 🕇	
3 Ge	nerate the rep	ort		,	•
4 Sa	ve the templat	e		,	•

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.



Report Builder			
1 Choose a templa	te		^
2 Modify the layou	t		^
<b>3</b> Generate the rep	ort		~
Date Range	<	October 30, 2022	>
File Subject	Daily Sec	urity Report	
	Save a	copy in the File Repository	
		Ge	nerate
4 Save the templat	te		^

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.

Report Builder		
1 Choose a temp	late	^
2 Modify the layo	but	^
<b>3</b> Generate the re	eport	^
<b>4</b> Save the templ	ate	~
Save Action	Create New Template	~
Template Name		
		Save



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.

List Of Schedules							۵
Portal Tag 🛛 + -	Report Template	t Interval	+ Enabled ++	Notifications *+	Date Created ++	Last Updated 👘 🗧	
	HIPAA Firewall and Server	Weekly		0	Sep 12, 2022	Sep 12, 2022	
	AP - Monthly Security Report	Monthly		2	Feb 9, 2022	Feb 9, 2022	
	Monthlu Security Dunning	Monthly			0++25 2021	0+ 25 2021	

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 <u>Contacts</u> should receive notifications when this report is generated. When done, select the Save button.

Schedule Report	
Report Template 🔆	
CB report	~
Enabled <b>*</b> Yes	
Contacts	
Customer	÷
	Save

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, <u>create a support ticket</u> to make add/edit/delete requests or to request additional permissions.

Assets	1. <u>Users</u> – Individuals authorized to log in to the Lightning Portal.
Users Contacts Devices	<ol> <li><u>Contacts</u> – 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).</li> </ol>
Agents Groups Figure 56: Assets Feature Options	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.
	<ol> <li><u>Devices</u> – Includes all devices sending logs into the Lightning Portal.</li> </ol>
	<ol> <li><u>Agents</u> – Applications installed on endpoints to allow monitoring.</li> </ol>
	<ol> <li><u>Groups</u> - Displays groupings of devices (ex: network devices, New York office servers, testing, etc.).</li> </ol>

Assets > Users

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

Users Search			()	No filters are applied, all result	s are	shown.				e,
List Of Users										
Portal Tag 🔷 +	User Name	Full Name		Email Address		Authentication	Enabled 🕆	Date Created	Last Updated	
	-					Portal Authentication		Jun 8, 2022	Jun 8, 2022	
					1	Portal Authentication		Nov.2, 2022	Nov.2, 2022	
						Portal Authentication		Jun 8, 2022	Jun.9, 2022	

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
FullName	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.

Users Search		e,
	No filters are applied, all results are shown.	
Portal Tag	Ŷ	
Username		
Full Name		
Email Address		
Roles	×	
Enabled	~	
	Search	

Figure 58: Users Search

### Add User

To add a User, select the Add icon and 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, <u>create a support ticket</u> to request an additional User account.



		14 Te
Edit	1.	<b>User Name</b> – choose a unique username for each User
User Name 🗚 🛈		account
	2.	Full Name – input first and last name for the User
Full Name 🗰 🛈	3.	Email Address – input the email address associated
Email Address 💿		with the User account
	4.	Receive Bulletins – check the Yes box for this user
Receive Bulletins		account to receive Bulletins
Time Zone	5.	Time Zone – choose the appropriate time zone
-	6.	Language – choose the appropriate language
Language	7.	Authentication – choose the appropriate
 Authentication <b>*</b>		authentication option (Portal or Lightweight Directory
Portal Authentication		Access Protocol (LDAP))
Second Factor	8.	Second Factor – choose the appropriate second factor
-		option
Enabled Yes	9.	<b>Enabled</b> – check the Yes box to enable this User
Roles *		account, uncheck the box to disable the account
Customer Administrator Customer User Handle Incidents Manage Contacts Manage Devices Manage Files Manage Portals Manage Tickets	10.	<b>Roles</b> – Select a role for this user account, use the CTRL key to select multiple options
Figure 59: Add User Screen		

### **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, <u>create a support ticket</u> to request edits.

Andrew	2 🔒
Enabled	
Ves	
Time Zone	
Language	
Login Portal	
OutSOC	
Authentication	
Portal Authentication	
Second Factor	
Roles	
Customer Administrator	
Customer User	
Handle Incidents	
Manage Brands	
Manage Contacts	



### **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 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.

Change Password	Password Restrictions
New Password 🗚	<ul> <li>Password must be between 8 and 70</li> </ul>
•••••••	characters
Confirm Now Dessword M	• Password must contain at least 1 letter,
	1 number, and 1 special character
P	Password may not be the same as or
Cancel Save	contain the username
	Suggested temp password:
	an\$Ej2YTE

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).



Authentication 米
Portal Authentication
Second Factor
Enabled
✓ Yes
Roles 🜟
Customer Administrator Customer User Handle Incidents Manage Contacts

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

Note: Having a <u>User</u> 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.

Contacts Searc	h No filters are applied, all results are sho	wn			X	٩
List Of Contact	5					
Portal Tag 👎 🗉	Name * - Email Address List		Enabled 👘	Date Created	Last Updated	
	ADD-CC			May 6, 2022	May 6, 2022	
	Sysadmins			Dec. 30, 2020	Jun 24, 2022	
				May 16, 2022	May 16, 2022	
	IT Salf			Aug 3, 2022	Aug.3, 2022	
	Customer			May 18, 2022	Jun 14, 2022	
				Aug 25, 2022	Sep 8, 2022	
				May 18, 2022	Sep 8, 2022	
				May 24, 2022	May 24, 2022	
				Aug 24, 2022	Aug 24, 2022	

*Figure 63: Assets > Contacts Functionality* 

Figure 62: Edit User Window Assets > Contacts



### **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.

Contacts Search	
	No filters are applied, all results are shown.
Portal Tag	~
Name	
Email Address	
Enabled	~
	Search

### 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 64: Contact Search Criteria



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

SILVERSKY

- 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 <u>Playbook</u> 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 <u>Playbook</u> 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.



DD-CC     Email Address List     Email Format   HTM   Roceive Bulletins   No   8000 1.800 America (Chicago   Phone Number (During Business Hours)	Contact				2/
Email Address List Email Format: TMU: Roceve Bulletins: No Mous Bool: 1830 America/Chicago: Phone Number (During Business Hours) Phone Number (After Business Hours) Phone Number (After Business Hours) The mail of the Business Hours) The Business Hour	ADD-CC				
Email format HTNL Receive Bulletins No Hours 800 - 18:00 America/Chicago Phone Number (After Business Hours)  Phone Number (After Business Hours)  Enabled Yes Date Created May 6, 2022 at 4:07:07 PM EDT Last Updated May 6, 2022	Email Address List				
Receive Buildeins   No   Boo 1   Boo 3   Boo 1   Boo America/Chicago   Phone Number (During Business Hours) Phone Number (After Business Hours) Panoe Number (After Business Hours) </td <td>Email Format HTML</td> <td></td> <td></td> <td></td> <td></td>	Email Format HTML				
Hours   B00 - 18:00 America/Chicago   Phone Number (During Business Hours)	Receive Bulletins No				
Phone Number (During Business Hours)   Phone Number (After Business Hours)     Language     Enabled   Yes   Date Created   May 6, 2022 at 4:07:07 PM EDT   Last Updated   May 6, 2022 at 4:07:07 PM EDT	Hours 8:00 - 18:00 America/Chicago				
Phone Number (After Business Hours)   Ianguage   Ianguage   Tenabled   Yes   Date Created   May 6, 2022 at 4:07:07 PM EDT   Last Updated   May 6, 2022 at 4:07:07 PM EDT	Phone Number (During Business Hours) 				
Language Tenabled Yes Date Created May 6, 2022 at 4.07:07 PM EDT Last Updated May 6, 2022 at 4.07:07 PM EDT Playbook Hours + Level + Status + Classification + Group + Action +	Phone Number (After Business Hours)				
Enabled   Yes   Date Created   May 6, 2022 at 4:07:07 PM EDT     Playbook     Hours   ++   Level   ++ </td <td>Language</td> <td></td> <td></td> <td></td> <td></td>	Language				
Date Created May 6, 2022 at 4:07:07 PM EDT         Last Updated May 6, 2022 at 4:07:07 PM EDT         Playbook         Mours       + + Level       + + Status       + + Classification       + + Group       + + Action       + + Action       + + Action       + + + Action       + + + Action       + + + + Action       + + + + + + + + + + + + + + + + + + +	Enabled Yes				
Last Updated May 6, 2022 at 4:07:07 PM EDT         Playbook       Playbook         Hours       ++ Level       ++ Status       ++ Classification       ++ Group       ++ Action       ++         No data available in table       No data available in table       ++       ++       ++       ++	Date Created May 6, 2022 at 4:07:07 PM EDT				
Playbook	Last Updated May 6, 2022 at 4:07:07 PM EDT				
Playbook     Playbook       Hours     ++ Level     ++ Status     ++ Classification     ++ Group     ++ Action     ++       No data available in table					
Hours ++ Level ++ Status ++ Classification ++ Group ++ Action ++ No data available in table	Playbook				2
No data available in table	Hours ++ Level ++ Status	++ Classification	÷÷ Group	++ Action	
		No data available in table			

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 22 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 .

Hours ↑↓ Level ↑↓ Sta	atus ↑↓ Classification ↑↓	Group ↑↓ Action ↑↓	
Any Any Re	viewed Any	Any 🖸	

### 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



Edit Customer	
Hours	
	~
Level	
	~
Status	
	~
Classification	
	~
Group	
	~
Action	
	~
Cancel	Add Playbook

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.

Devices Search	No filters are applied, all results are shown.							
List Of Devices Portal Tag  Portal Tag Porta	<ul> <li>Name</li> <li>MGD-192.168.236.39</li> <li>MGD-AF-F1-HA_FG5H1E</li> <li>MGD-avfg-collector-1</li> </ul>	Vendor Product IP Address CentOS Linux Fortinet FortiGate Fortinet FortiSIEM	Status Enabled active	Date Created         Last Updated           Jun 8, 2022         Jun 30, 2022           May 24, 2022         Jun 22, 2022           May 24, 2022         Jun 22, 2022				

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.

Devices Search	
	No filters are applied, all results are shown.
Portal Tag	~
Device Tag	
Name	
Vendor Products	~
IP Address	
Status	~
Enabled	
	Search

Figure 71: Device Search Criteria

### Add a Device

To add a Device, select the Add icon **C** 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 <u>create a support ticket</u> to request a device be added.

	R I
Edit	1. Device Label – Enter a descriptive label for the
	2. Device lag – Enter a device tag by which the
	device will identified in incoming streams of
	logs and alerts
Vendor Product *	3. Vendor Product – Enter the device
3Com TippingPoint Security Management System	manufacturer, model, and version
Group	4. <u>Group</u> – Enter the Group to which the device
	belongs, if applicable (ex: West Region
Description ①	Firewalls)
	5 Description - A human readable description
	5. Description – Anumameadable description
Status	of the device, what it is used for, and any
New	additional nelptul notes
Enabled *	<ol><li>Status – Choose from the options: New,</li></ol>
✓ Yes	Deployment, Tuning, Active, or Cancelled
Serial Number 💿	7. Enabled – Check the box to enable. Note:
	disabled devices won't trigger incidents
FQDN O	8. Serial Number – Unique identifier from
	manufacturer
MAC Address 💿	6 EODN - Fully Qualified Domain Name
IP Address 🛈	10. MAC Address
Figure 72: Add Device Criteria	11. IP Address
igare 72. Add Device Ontena	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.

SILVERSKY



00-Backup	2
00-Backup. Wazuh Agent for Windows	
Group	
Description	
Enabled	
Yes	
Status	
Active	
Serial Number	
FQDN	
MAC Address	
IP Address	
NAT IP Address	
Date Created Sentember 20, 2022 at 8-57-06 AM FDT	
DateUpdate	
2022-37-03123-00-30	

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 a 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.





### **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.

Agents Search	<b>h</b> ] 1		No filters	are applied, all results a	re shown.		÷.	م
List Of Agents Portal Tag	; Device Tag	Name		Vendor Product 👓 🕫	Version *+	Operating System 🔹 Status 🔹	Last Updated	•
-	SENTINELONE- Workstations_Limited			SentinelOne Endpoint Protection Service	22.1.4.10010	Windows 10 Pro 19044	2022-08-03 13:19:04	
-	SENTINELONE-I	_		SentinelOne Endpoint Protection Service	21.5.4.291	Windows 10 Pro 19043	2021-09-09 13:43:39	
	SENTINELONE- Workstations			SentinelOne Endpoint Protection Service	22.1.4.10010	Windows 10 Education 19042	2022-08-16 01:34:40	

*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.

Agents Search		
	No filters are applied, all results are shown.	
Portal Tag		~
Device Tag		
Name		
Vendor Products		~
	Search	

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.)

Groups Search		No filters are applied, all results are shown.	۹
List Of Groups			÷
Portal Tag	to Name	++ Description	Last Updated
	Domain Controllers		2022-09-16 21:06:10
			2022-10-03 15:22:12
			2022-10-14 15:12:25
		List of all Servers	2022-10-03 20:17:51
		Group for all storage related products, such as NetApp.	2022-08-22 20:17:28
		Demo	2022-09-02 13:54:08
			2022-09-23 15:20:41
		Group Description. Test.	2022-10-06 13:58:11

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

Groups Search	
	No filters are applied, all results are shown.
Portal Tag	~
Name	
	Search

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 <u>Edit Device</u> window. If a User account does not have the necessary permissions to add a Group, <u>create a support ticket</u> 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.



**Operations > Response Plan** 

The Response Plan is a read-only summary of the <u>Playbook</u> 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 CentOS Linux CentOS Linux Fortinet FortiGate Fortinet FortiSIEM



### **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	Апу	Any Send Notification					
Phone Su	oport							
To call with a	ny questions or esc	calations:						
(800)								
Response Analysts will	e <b>Times</b> handle incidents w	vithin the specified times:						
<b>1 Low</b> 1d	•o0	<b>2 Medium</b> 1d	3 High 10min	4 Critical 10min				



**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 B	List Of Bulletins								
Portal Tag		Bulletin ID 🔷 🖗	Title		Bulletin Type ↑↓	Date Created		Last Updated	
			Zero-day Vulnerabilities in Microsoft Exchange Server		Vulnerability	Sep 30, 2022			
			Release v2.7.0 - Workflow Changes and Device Groups		Feature Release	Aug 24, 2022			
			Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control		General Notice	May 18, 2022			
			Okta Investigating Possible Data Breach		General Notice	Mar.22, 2022			
			NCSC-NZ Releases Advisory on Cyber Threats Related to Russia-Ukraine Tensions		General Notice	Feb 24, 2022			
			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.



Notification Search									۹		
						2022-10-03 to 2022	11-02				
List Of No	tificat	ions									
Portal		Recipient Type		Recipient		Notification Type		Email Gateway	Status	Date Created	
		Contact		Customer		incident/updated			sent	Nov.2, 2022	
		Contact		Customer		incident/updated			sent	Oct 29, 2022	
		Contact		Customer		incident/updated			sent	Oct 28, 2022	

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	Input an email address
Address	
Status	Choose Sent or Attempted
Limit	Choose the max number of records to be displayed in the search results

Notification Search	
	2022-10-03 to 2022-11-02
Portal Tag	~
Date Range	2022-10-03 ~ 2022-11-02
Search Email Address	
Status	×
Limit	100 ~
	Search

Figure 85: Notifications Search



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

Audit Search			2022-10-03 to 2022-11	-02			Q
List Of Audits Origin Portal ++ Affected Portal ++	Resource ↑↓	Action **	Path		Performed By	Notes	
	Page Page Authentication	read read login	/manage/audits/ /manage/notifications/ /manage/notifications/				
	Page	read	/assets/contact/FFF06400-D6A9- 11EC-9731-DC6B822F99DF				

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

Audit Search	2022-10-03 to 2022-11-02
Portal Tag	~
Date Range	2022-10-03 ~ 2022-11-02
Resource	~
Action	·
Performed By	· · · · ·
Search	
	Search

Figure 87: Audit Search



Resource	~
Action	Alert Filter Alert Note
Performed By	API Key Authentication Brand
Search	Bulletin Contact
	Device File Page
	Report Schedule Sensitive Account
	Ticket Token Link Portal
	User

Figure 88: Audit Search: Resource

Management > Session Tracking

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

Logged-Ir	n Users	5						
Origin Portal		Username	Full Name	IP Address 🗠 🖗	Logged In	Last Seen	Duration 😁	Status 🤊
				_	November 2, 2022 at 2:31:18 PM EDT	November 2, 2022 at 3:02:31 PM EDT	31:13	🕌 online
		-			November 2, 2022 at 9:52:32 AM EDT	November 2, 2022 at 11:42:15 AM EDT	1:49:43	<b>A</b> offline

Figure 89. Management Session Tracking

### Resources

The Resources functionality provides access to files available for download.



Figure 90: Resources > Downloads



Dow	nloads
Co	lectors
-	ESXi
	Silversky Log Collector v1.0.2 Deployment Guide.pdf (598.3 KB)
	silversky-log-collector-v1.0.2.ova (787.8 MB)
-	HyperV
	Silversky Log Collector v1.0.2 Hyper-V Deployment Guide.pdf (380.5 кв)
	silversky-log-collector-hyperv-v1.0.2.zip (761.4 MB)
🖿 ED	R Agents
	Cylance
	Archive
	Dptics
	🖿 Mac
	3_0_1180_5000_CylanceOPTICS.pkg (54.4 MB)
	Protect
	🔤 Mac
	2_1_1590_512_CylancePROTECT.pkg (32.5 MB)
	2_1_1594_518_CylancePROTECT.pkg (33.0 MB)
	3_0_1000_511_CylancePROTECT.pkg (33.0 MB)
	Windows

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.