FAQ – Device Management & Monitoring Platform Upgrade

1. **Which customer portal will I use with our Device Management & Monitoring service(s)?**
    - Lightning Portal (aka outSOC) – This portal is for all alerts, cases, and communication with our SOC team
    - SMC—This portal is designed for managed device customers and will be used primarily for device audit logs, configuration changes, compliance, and executive summary reports.

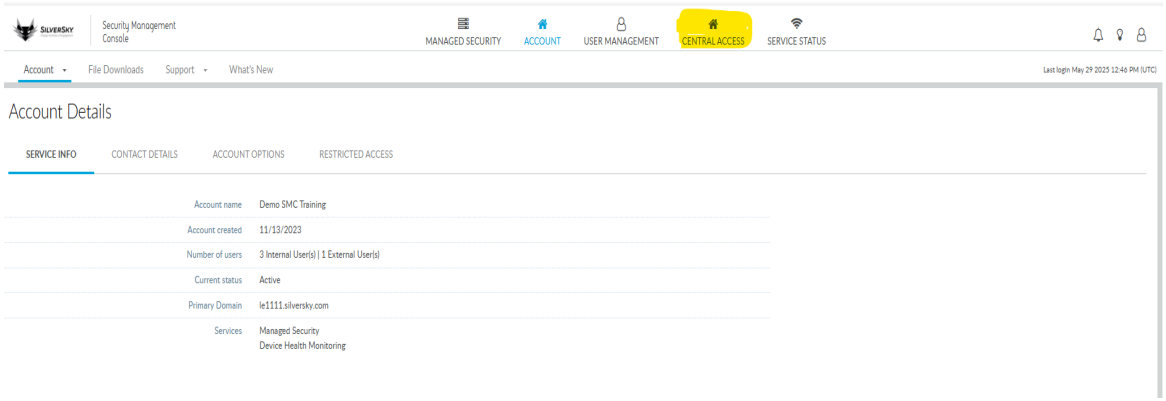
2. **Will SMC still have alerts and security activity updates?**
    - NO ** (you will still have access to previous alerts within SMC before your conversion date). All new alerts will be on the Lightning Portal

3. **Will I work with the same SilverSky team for support?**
    - YES

4. **When will this change take place?** May and June 2025

5. **Is there a Knowledge Center where I can get sample reports and instructions on how to use the new Lightning Portal?**
    - Device Management & Monitoring Platform Upgrade Knowledge Center - SilverSky

6. **How do I get credentials for the new Lightning Portal?**
    - You'll be able to log into the Lightning Portal using your current SMC credentials by logging into SMC Portal (cloud.postoffice.net). Select 'Central Access'.



- You'll be redirected to the Central Access Portal screen, and you must select '**Lightning Customer Portal (fka OutSOC)**'.

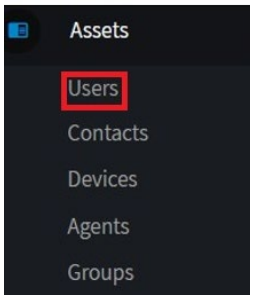
7. How do I change my password in the new Lightning Portal

- Passwords are managed within the SMC Portal; you must follow the steps for resetting passwords on SMC.

8. Who will be able to use the new Lightning Portal?

- All users who have the **MSS Admin** role in SMC today have been carried over to the Lightning Portal.
- NOTE: It's a good opportunity for you to review your access controls and make sure that the user list is still accurate for your organization

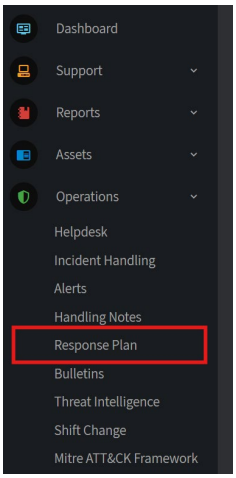
9. **How to add new users to the Lightning Portal?**
    - Follow page 39 (Assets ->Add Users) in the Lightning Portal Users Manual to create the user.
    - **NOTE: Any User added to the Lightning Portal must have a corresponding user account on the SMC Portal (cloud.postoffice.net) to enable the SSO capability to work**



10. **Will my role settings change?**
    - **MSSP Admin** access roles on SMC are the equivalent of **"Customer Administrator"** on the Lightning Portal.
    - Customers should review all of the Users and Contacts imported into Lightning Portal and verify that access is appropriate for their organization
    - If you want to change the roles for individuals in your organization, contact our SOC to do so at SupportDB@SilverSky.com

11. **What's the difference between Users and Contacts in the Lightning Portal?**
    - **Users** – Individuals authorized to log in to the Lightning Portal.
    - **Contacts** – Points of contact (individuals or group distribution lists) who receive notifications for incidents, support tickets, and reports. Contacts do not need to have a User account (ex, a senior leader may want to receive notifications and reports but does not need to log in to the Lightning Portal).

12. **Will my Response playbooks change?**
    - We have carried over the response plan configuration based on your current setup
    - Customers are encouraged to review their plans and make changes based on their business needs
    - Access Response Plans in the Lightning Portal from the Operations menu bar



- See page 45 in the Lightning Portal Users Manual to follow the steps to update the response plans on the Lightning Portal. Changes take effect immediately.

13. Will the Incident Handling Policy change?

- Yes.
- Customers will receive a new Incident Handling Policy during the migration process. The document will be available in the Lightning Folder in the Files folder

14. Are the Threat Intelligence feeds different?

- Yes. We will no longer be using IBM-xForce.
- We will be using Fortinet Threat Intel feeds along with new advanced threat feeds from multiple locations.

15. Will the Common Customer Alerts be different?

- Yes, this is known as “Handling Notes” in the Lightning Portal
- Customers' current “Common Customer Alerts” will be migrated to the new Lightning Portal as part of the migration process

16. Is the blocking process different?

- Yes, we were creating tickets in the past, and SilverSky engineers manually created blocks.
- With the new Lightning platform, SilverSky has automated thousands of known malicious IPs and sites through our Threat Feed Engine. Our managed device clients need no customer interaction to enable the Threat Feed

Engine once customers are on the Lightning platform. Monitor only clients need to provide us with IP address information (see the Threat Feed Engine document on our Knowledge Center).

- For clients with " auto-blocking not enabled," SilverSky recommends removing this flag and using the Threat Feed Engine.

17. Will the SIEM rules change with the move to the new SIEM technology?

- Yes.
- In the past, SilverSky created custom rules for clients upon request. The new technology uses advanced analytics and AI to respond to the rapid changes in the threat landscape. Customers may still request additional blocks, but most of the rules and coverage will be from the technology itself.

18. Will auto-generated rules be in place on the new platform?

- No
- Clients can now enable "auto notifications" depending on their preference for topics to notify. This is done in the Lightning Portal; see page 54 in the Lightning Portal Users Manual for additional information.

19. Will I still get Compliance Reports in SMC?

- Yes, however, they will not include alert activity.
- You may run Lightning Portal reports, which provide an Executive Summary of the alert activity that can accompany your Compliance Report