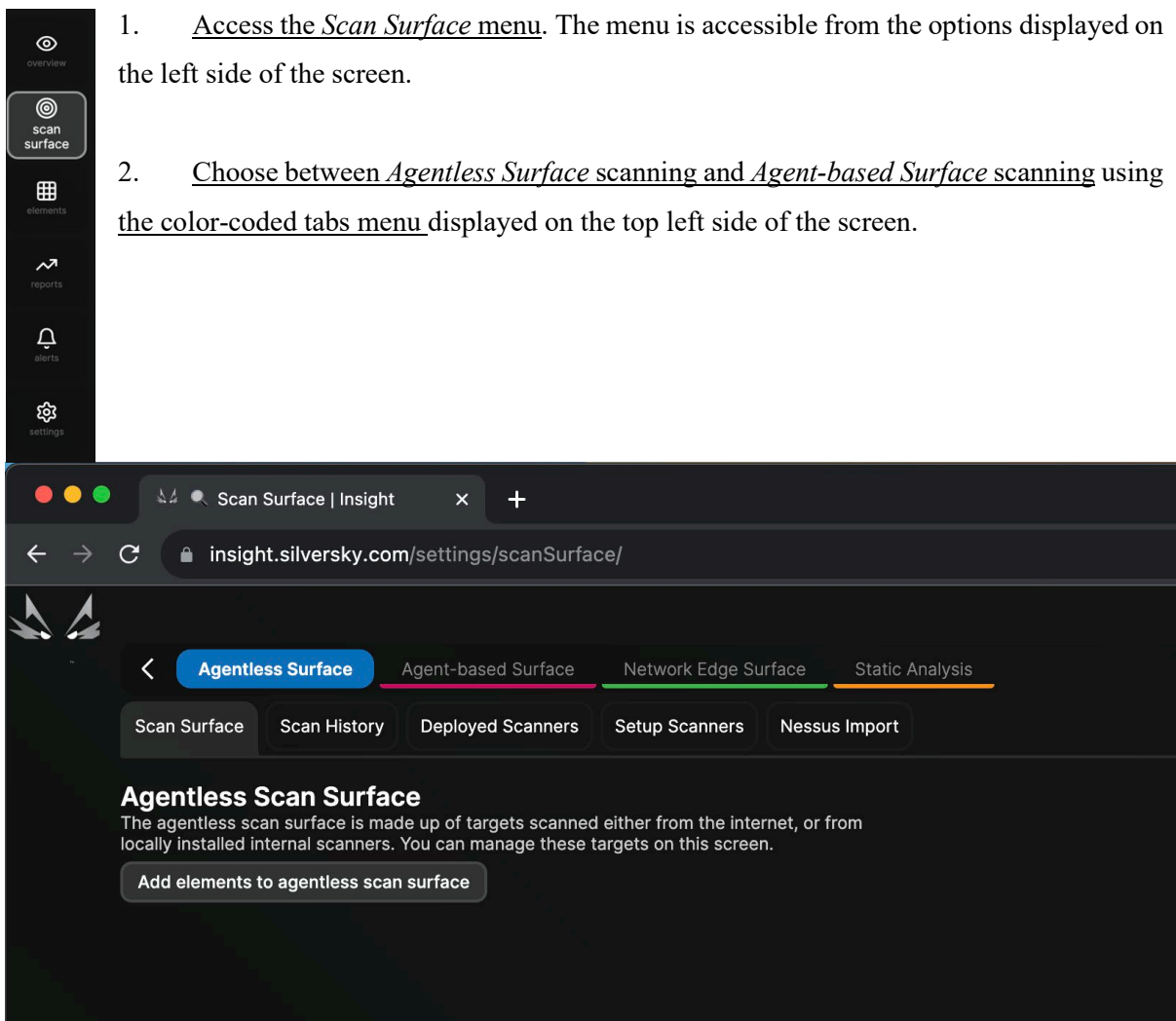


How To Guide – Running Your First Scan

This guide presents the steps required to run your first cybernetic vulnerability scan using the Insight portal at <https://insight.silversky.com>



The screenshot shows the SilverSky Insight portal interface. On the left, a vertical navigation menu contains icons for 'overview', 'scan surface', 'elements', 'reports', 'alerts', and 'settings'. The 'scan surface' icon is highlighted. The main content area shows the 'Scan Surface | Insight' browser tab and the URL 'insight.silversky.com/settings/scanSurface/'. Below the navigation bar, there are four tabs: 'Agentless Surface' (selected), 'Agent-based Surface', 'Network Edge Surface', and 'Static Analysis'. Underneath, there are sub-tabs: 'Scan Surface', 'Scan History', 'Deployed Scanners', 'Setup Scanners', and 'Nessus Import'. The 'Agentless Scan Surface' section is active, displaying the title 'Agentless Scan Surface' and a description: 'The agentless scan surface is made up of targets scanned either from the internet, or from locally installed internal scanners. You can manage these targets on this screen.' Below the description is a button labeled 'Add elements to agentless scan surface'.

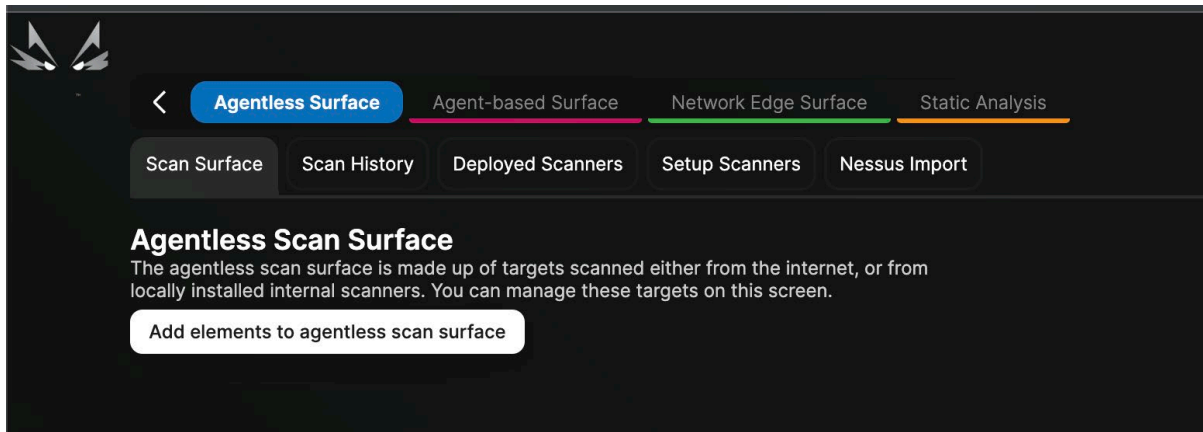
1. Access the *Scan Surface* menu. The menu is accessible from the options displayed on the left side of the screen.
2. Choose between *Agentless Surface* scanning and *Agent-based Surface* scanning using the color-coded tabs menu displayed on the top left side of the screen.

- I. *Agentless Surface* scanning involves detecting cyber vulnerabilities in your infrastructure without the need to install any software program. It is less resource-intensive but also less accurate than the Agent-based scan.

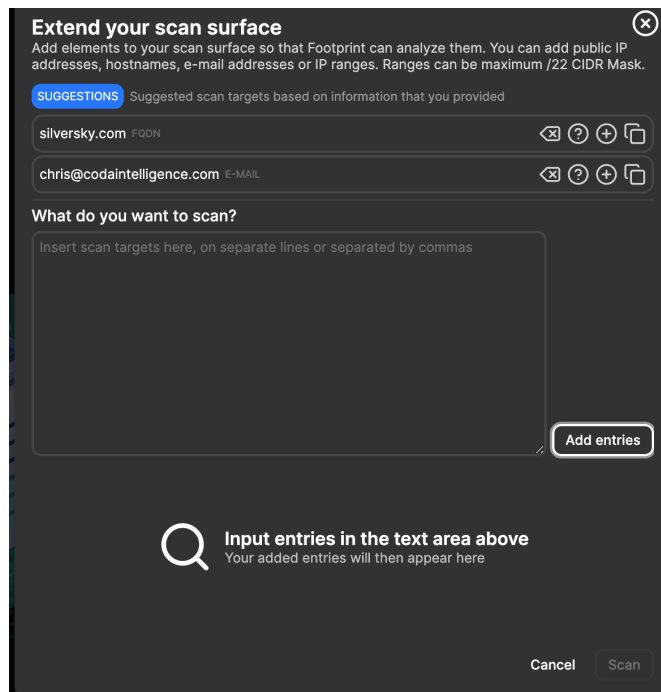
- II. *Agent-based Surface* scanning involves detecting cyber vulnerabilities in your infrastructure by installing a software program. It is more resource-intensive but also more accurate than the Agentless scan.

Section I. Running your first Agentless Surface scan

After selecting the *Agentless Surface* scanning tab, follow the next steps for running the scan:



1. Click on the *Add elements to agentless scan surface* button placed on the top left of the Agentless Surface page. This action will open a pop-up in which you can configure the scan.

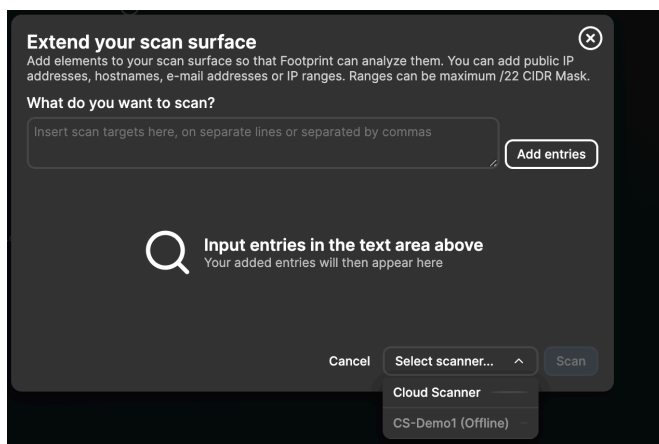


2. Write the elements that you want to scan in the text field of the pop-up. Click on the *Add entries* button placed on the right of the text field after writing the elements. The elements can be public or private IP addresses, hostnames, e-mail addresses, and IP ranges.

When adding multiple elements in the text field, you should write them one below another.

!An IP range can be defined using the following format: 192.168.10.0/24. It helps you avoid writing each IP individually.

3. Choose between the *Cloud Scanner (default)* or an *Internal Scanner* using the dropdown placed in the bottom right of the pop-up form.



It is possible that no Internal Scanner option is displayed. This is because Internal Scanners must be set up (see point b. below)

- a. *Cloud Scanner (default)* involves detecting cyber vulnerabilities using an outside-in approach. This type of scanning is adequate when your elements are accessible by a public IP (e.g., a website)

It is possible for the public IP of the Cloud scanner to be blocked by the Firewall of your infrastructure. As such, you may have to add it to the Firewall whitelist. Check the *Deployed Scanners* sub-tab (accessible from below the color-coded tab menu placed in the top left of the *Agentless Surface* tab) to get the public IP of the Cloud scanner.

- b. *Internal scanning* involves detecting cyber vulnerabilities using an inside-out approach. This type of scanning is adequate when your elements are not accessible by a public IP (e.g., internal network, VPN, cloud)

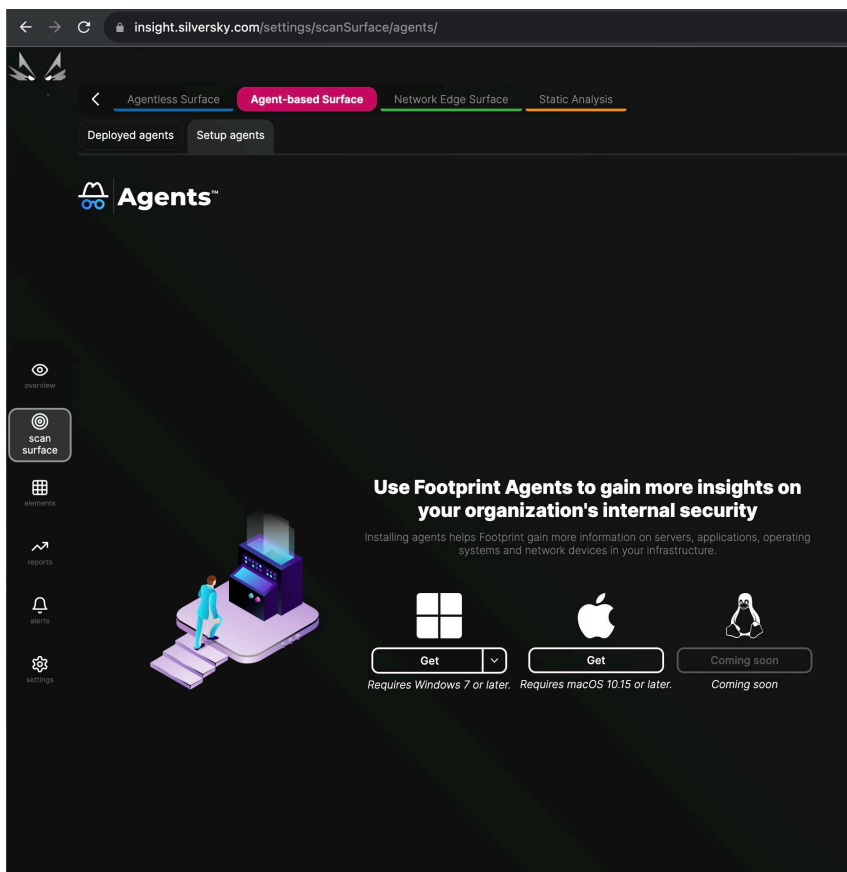
We recommend setting your first Internal Scanner during the Agent-Based scan (see Section II, step 2. b). You can also set it up from the *Setup Scanners* sub-tab (which is next to the *Deployed Scanners* sub-tab).

4. Press the *Scan* button. A progress pop-up will be displayed afterward. The scan may take between 2 and 10 minutes for one IP address. You can minimize the pop-up or choose to stop the scan. When finished, you can analyze the scan results.

After minimizing the pop-up, the progress bar will be displayed in the top left corner of the screen. Pressing the “X” button on the latter bar will stop the scan.

Section II. Running your first Agent-based scan

After selecting the Agent-based Surface scanning tab, follow the next step:



1. In the *Setup agents* sub-tab (accessible from below the color-coded tab menu placed in the top left of the screen) get the executable for installing the agent by clicking the button *Get* for the appropriate operating system.

2. Run the installation after the executable is downloaded:
 - a. Read the terms of the license agreement and press *I Agree*
 - b. Choose whether to install an Internal Scanner by checking the associated box and press *Next*.

If the option to include an Internal Scanner is checked, a pop-up will display. It will ask you to be sure that your CPU allows the creation of virtual machines (virtualization is enabled). Additionally, be sure to have at least 12GB RAM, 2VCPUs, and 100GB of disk space. Press *OK* and allow the installation software to check if you have these requirements.

- c. Choose the installation folder and press *Next*.
 - d. Choose whether to perform the Agent-based scanning on the current computer or the computers connected to an Active Directory.
 - e. Fill in the connection details. These are available on the right side of the *Setup agents* sub-tab from where the installer was downloaded (see step 1).

The Root CA certificate location is not needed unless an SSL inspection is required.

- f. Press *Install*, wait for the Agent to be deployed, and then press *Finish* after the installation has ended.
3. Check if the Agent was successfully deployed on the *Deployed agents* sub-tab (placed next to the *Setup agents* sub-tab).

As soon as the agent is installed it will start scanning. This may take a few minutes after the installation is completed. The Last Update field in the table from the *Deployed agents* sub-tab will be updated as soon as the agent finishes its first scan.

If the option to install the Internal Scanner was opted for, please check if it was installed in the *Deployed Scanners* sub-tab from the *Agentless Surface* color-coded tab. The Internal Scanner should have a similar name to that of the Agent.