Outpost24

Vulnerability Management made easy

Scanning Less Scanning

A Setup Guide

Version: 2.2

2018-06-20

Table of Contents

About this Guide

The purpose of this document is to assist users when installing and configuring Scanning-Less Scanning (SLS) available for Outpost24 products. This document has been elaborated under the assumption that the reader has access to the OUTSCAN/HIAB account and Portal Interface.

For support information, visit https://www.outpost24.com/support.

1 A Traditional Approach

Traditionally, organizations use vulnerability management tools to scan their network at regular intervals. This includes daily, weekly, bi-weekly, monthly, bi-monthly and quarterly intervals. If a new vulnerability is discovered in between those scans, the system is unknowingly susceptible to an attack during that time.

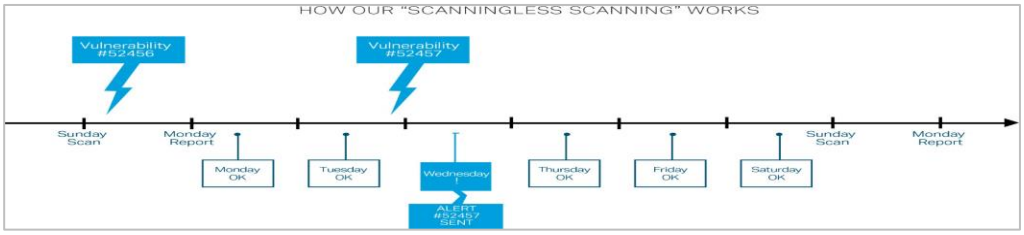
Traditional vulnerability management tools provide organizations with a false sense of security between regularly scheduled scans. The organization may feel safe, but new vulnerabilities during the time period between scans can be exploited to cause significant losses

2 Outpost24's Unique Approach - SLS

In striving to offer a more proactive approach to vulnerability management, Outpost24 has incorporated a unique tool feature called **SLS**, which decreases the overall exposure window for attacks and eliminates risk.

When a new vulnerability is discovered, Outpost24's products are immediately updated. The tools then compare information gathered during the last scan and alert the user about any systems that could be affected by this new vulnerability.

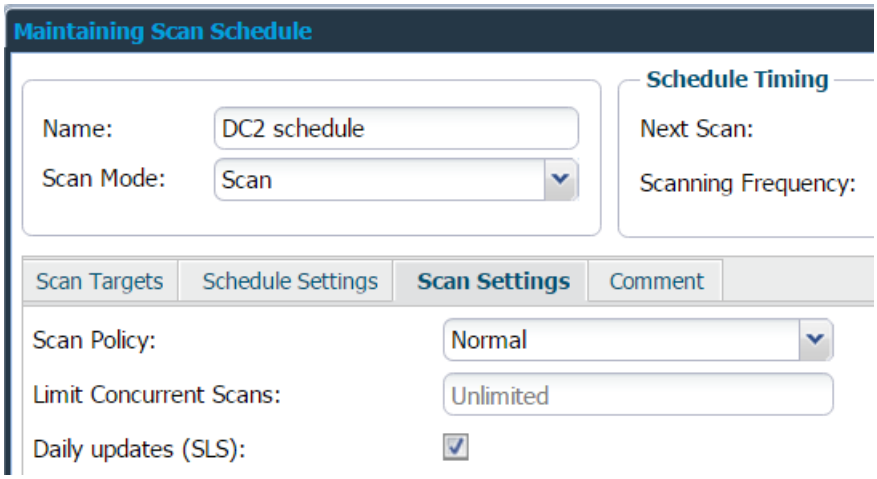
SLS is included in OUTSCAN, an on-demand Software-as-a-Service, and HIAB, a plug and play appliance, both of which allow organizations to easily detect vulnerabilities and manage remediation to prevent hackers from penetrating the network. Below figure shows how our **Scanning-Less Scanning** works.



3 Enabling Scanning-Less Scanning

To enable the **SLS** feature on your scans, follow the below steps.

1. Go to **Menu**
2. Click on Target Scanning, select Scan Scheduling.
3. Select a specific schedule and right click on the schedule name.
4. Select the **Edit** option from the context menu. This displays the **Maintaining Scan Schedule** window.



5. Select the **Scan Settings** tab as shown in the above figure.
6. Select the option **Daily updates**. This is the Scanning-Less Scanning feature, which allows the report to be updated daily (at the same time of day that is defined in the **Next Scan** field) with any new vulnerability that may affect the specific system.

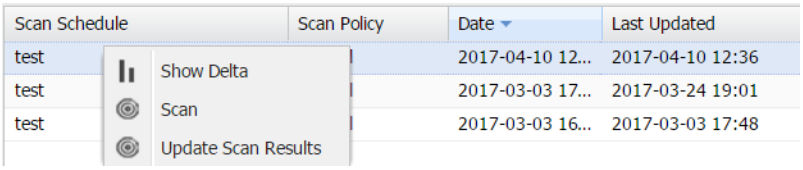
Note: *The fingerprint database for a system will only be retained for a maximum of one month. After that period, the fingerprint database will be considered outdated and no longer be used.*

3.1 Ad-Hoc Scanning-Less Scanning

It is also possible to perform manual Scanning-Less Scans whenever needed.

To perform manual Scanning-Less Scan:

1. Go to Reporting Tools
2. Right click on a schedule and select **Update Scan Results**.



This initiates a Scanning-Less Scan against the target and compare new vulnerabilities with the fingerprint stored for this scan. Any new vulnerability that is added through a SLS scan can be identified in the **Findings** grid, **Added** column. The new findings will be available in the same report with a different date in the column **Date Added**, which can be added to the **Findings** grid.
SLS can also be initiated from a single target through **Target** section under **Reporting Tools**.

Note: *If the report does not have a valid fingerprint database stored, this option won't be available in the above menu. In other words, this option will only be available on latest successful scan of the scan schedule.*

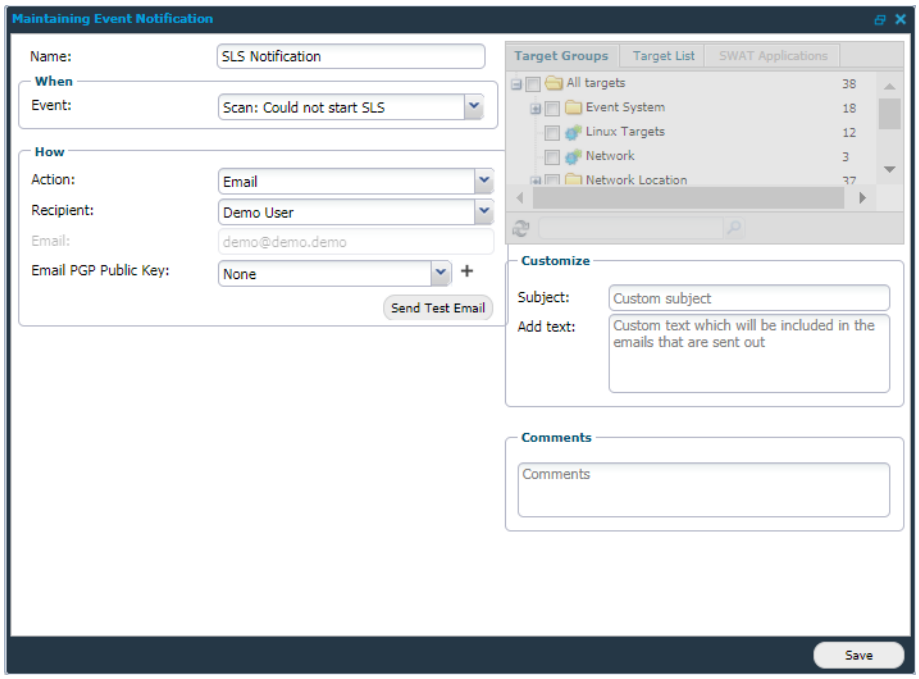
3.2 Automatic Notifications

You can receive alerts about SLS, or notify someone when a report is updated after SLS, or if the system is unable to start an SLS update.

To set the notifications:

1. Go to **Main Menu.**
2. Select **Event Notifications** under **Settings**.
3. Select **New** or right click on any entry and select **Edit**.

Note: *You should enable this feature only after the execution of an initial scan.*



In the above example, an email alert will be sent to the **demo user** whenever the system could not start SLS.

Note: *For more details regarding event notifications, please check Event Notifications guide.*