Lockpath

QualysGuard® LockPath Keylight™ Integration Guide

Keylight can dynamically pull in the latest vulnerability results from the QualysGuard Detection API. After configuring the Qualys API Scan settings, Keylight will begin synchronizing vulnerability data from the QualysGuard Detection API. Once the initial synchronization is complete, differential scan synchronizations will be performed automatically on a scheduled interval.

> **Note:** The QualysGuard user ID used to configure the QualysGuard API Scan settings must have API access and knowledge base access. It is recommended to ensure that at least three concurrent API sessions exist (one knowledge base, one API, and one for the user to log into the Qualys web pages).

Steps to configure the Qualys API Scan settings in Keylight:

1. In the **Setup** area of Keylight, open the **Qualys** connector and click **Edit**.
2. Enter the **API URL**, **API Username**, and **API Password** credentials provided by Qualys.
3. Enter the **KnowledgeBase Username** and **KnowledgeBase Password** credentials provided by Qualys for the knowledgebase download.

> **Note:** The credentials from Qualys must have permission to download the information from the QualysGuard API.

4. Configure the **Device Resolution** order to set the hierarchy for how devices discovered in a Qualys vulnerability scan are matched to devices in an assets table.
5. Next to **Import Vulnerabilities via Qualys Automatic Detection API**, select **Yes** to enable Keylight to dynamically pull in the latest vulnerability results from the Qualys Detection API. If set to **No**, Qualys network vulnerability scan files will need to be manually imported.
6. If **Import Vulnerabilities via Qualys Automatic Detection API** was set to **Yes** in step 5, continue with this step. Otherwise, skip to step 7. In the **Custom search string** field, type any desired filter parameters to restrict what hosts are imported into Keylight.

> **Helpful Hint:**
> - For example, the search string **qids=38140&severities=2,3,4,5** will retrieve the hosts that are found to be vulnerable with QID 38140 - SSL Server Supports Weak Encryption Vulnerability, but exclude those with a severity level of "Minimal."
> - If the search string **status={New,Active,Re-Opened,Fixed}** isn't entered, no vulnerabilities with a status of "Fixed" will be retrieved. Only vulnerabilities with a status of "New," "Active," or "Re-Opened" will be retrieved.

> **Note:** The following filter parameters are not supported:
> - action={list}&
> - vm_scan_since={date/time}&
> - no_vm_scan_since={date/time}&
> - output_format={XML|CSV|CSV_NO_METADATA}&
> - truncation_limit={value}&

7. Next to **Import Asset Groups via Qualys Automatic Detection API,** select **Yes** to enable Keylight to dynamically pull in the Qualys Device details, such as the Qualys Asset Group, for each plugin. Otherwise, select **No**.

8. Next to **Synchronization starting point**, a date and time to begin the dynamic synchronization of vulnerability data pulled from the QualysGuard API into Keylight can be manually set. Click the calendar icon and then select a date. Click the clock icon and then select an hour of the day.

9. In the **Severity mapping** section, using the drop-down lists in the **Keylight Label** column, specify which label (**Critical**, **High**, **Informational**, **Low**, **Medium**) to apply to each Qualys Score.

10. A remediation status can be automatically applied to all Qualys vulnerability scans with a particular severity score. In the **Auto Apply** column, click the drop-down list corresponding to the severity score to which a remediation status is to be applied. From the **Auto Apply** drop-down list, select a remediation status.

11. Click **Save**.

Qualys API Scan settings in LockPath Keylight