

FAQ – Asset Inventory Service

Welche Unterschiede bestehen zwischen den AddOns „Asset Inventory Service“ und „Anlagenstatus“?

Das bestehende AddOn „Anlagenstatus“ liefert Informationen über verbaute Hardware (inkl. weiterführende Informationen wie Firmware-Version, etc.). Hierfür werden die Daten bzw. Informationen im Zuge der konfigurierten Uploads gesammelt. Sind keine Uploads konfiguriert, liegen im Anlagenstatus keine entsprechenden Geräteinformationen vor.

Über den Asset Inventory Service sind weitere Informationen (verbaute Baugruppen, etc.) bzw. Vulnerabilities verfügbar und die Informationen werden nicht nur bei den Uploads gesammelt, sondern auch wenn eine neue Version einer Komponente auf das versiondog Serversystem eingecheckt werden. Außerdem wird eine größere Anzahl an Gerätetypen unterstützt.

Darüber hinaus ermöglicht der Asset Inventory Service eine Ergänzung der Daten durch Scannen des Netzwerks und gleicht alle Assets mit einer CVE Datenbank ab, so dass man direkt sieht, welches Asset von welchen Schwachstellen betroffen ist.

Weiterführende Informationen über die Scanfunktionen von Claroty bzw. dem Asset Inventory Service:

Seitens der hinterlegten Funktionalität von Claroty gibt es 2 Möglichkeiten, wie das vorhandene Netzwerk gescannt werden kann:

- **Passiv**
Über eine eigene Hardware-Box, welche an einem Switch des entsprechenden Netzwerk-Segments angeschlossen ist, wird der Netzwerkverkehr mitgelauscht bzw. protokolliert. Der passive Scan ist nicht im Lieferumfang enthalten und kann auch nicht bei AUVESY, sondern nur bei Claroty selbst hinzugekauft werden.
- **Aktiv**
Es wird ein aktiver Scan im hinterlegten Netzwerksegment durchgeführt, hierbei sind unterschiedliche Query-Konfigurationen möglich, sodass gezielt nur eine entsprechende IP-Range abgefragt wird oder eine Broadcastanfrage an das komplette Segment gestellt wird. Zusätzlich lässt sich auch die Abfragemethodik (z.B. Pingsweep) entsprechend konfigurieren.

Wie erfolgt der initiale Import bereits vorhandener Komponenten / Assets in das System?

Den initialen Import bereits bestehender Komponenten würden wir im Zuge des Einrichtungstermins gemeinsam mit Ihnen durchführen. Dieser Importvorgang kann initial einen etwas längeren Zeitraum in Anspruch nehmen. Hierbei wird zunächst kein Scan des Netzwerks durchgeführt, sodass eine Belastung des Netzwerks vermieden wird. Die Daten werden über eine bestehende Importfunktion „AppDB“ in das Claroty-System importiert. Zukünftige Anpassungen / Änderungen an den Assets werden dann automatisch im Hintergrund transferiert.

Welche Geräte / Systeme werden vom Asset Inventory Service erkannt?

In der Regel werden alle verbaute Assets erkannt, hierbei ist es unabhängig davon ob die Geräte z.B. per Profinet oder Profibus angeschlossen sind. Somit können auch „Nested“ Devices erkannt werden.

FAQ – Asset Inventory Service

Wie werden aktuelle Schwachstellenmeldungen der Hersteller (z.B. Veröffentlichungen von Siemens) zur Prüfung zur Verfügung gestellt, wenn kein Online-Zugang vorhanden ist?

In regelmäßigen Abständen (Vierteljährlich, in dringenden Fällen auch azyklisch) werden von Claroty Updatepakete für die jeweiligen Server angeboten, sodass auch neuere Schwachstellenmeldungen mit einem geringen zeitlichen Verzug auf dem System vorhanden sind.