ServiceNow Integration Overview

Asset Manager integration has passed ServiceNow's rigorous certification process and is available now in the ServiceNow Store. Search for "FireMon" or "Asset Manager" to get started.

In this implementation, Asset Manager highlights missing network data for the ServiceNow. ServiceNow then pulls this network data from Asset Manager. Cloud Discovery (aka Scanner) enables ServiceNow to pull cloud details from Asset Manager as well.

Here's how the integration works:

1. ServiceNow initiates the first API call to Asset Manager requesting a list of all third-party integrations configured on the Command Center and the connection status of each. This screenshot shows the scheduled job that calls the underlying API to pull data from Asset Manager.
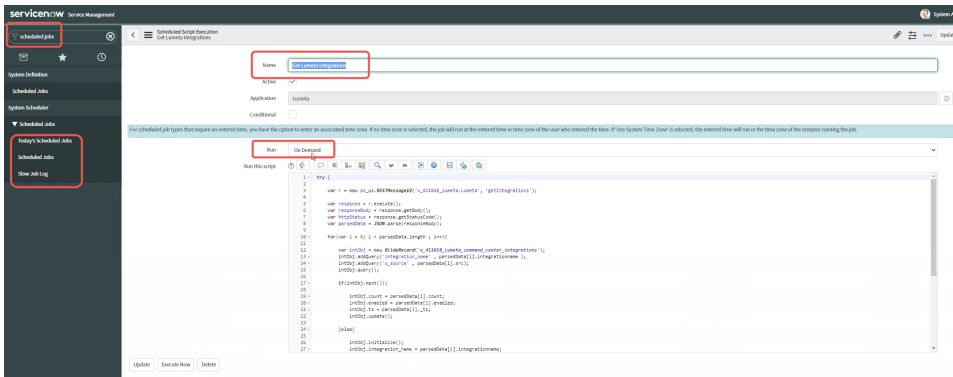
The results display in this Security Integrations dashboard in ServiceNow. It lists bundles of all third-party integrations configured on the Command Center and the connection status of each.

2. ServiceNow initiates a second API call to Asset Manager to see the gaps. Asking the question, "What does Asset Manager know that ServiceNow doesn't?"

   a. Did Asset Manager identify a device lacking an agent such as McAfee or Carbon Black
   b. Did Asset Manager find a device that ServiceNow hasn't scanned? (Tenable, Qualys, Rapid7)?
   c. Did Asset Manager discover a CIDR or IP that ServiceNow isn't aware of (Infoblox, BlueCat).

3. For those whose "SNOW Status" is unmatched, ServiceNow generates an incident ticket—one incident ticket per third-party vendor such as McAfee and containing individual records for each finding (e.g., one row for each of the device at issue).

4. ServiceNow security professional remediates the issue and marks the ticket as "completed."
5. ServiceNow initiates a third API call to Asset Manager to get an updated list of gaps.
6. Asset Manager compares the current issue-status to the expected issue-status to validate that ServiceNow-fixed issues are demonstrably fixed.
7. Asset Manger updates ServiceNow with the new status.

8. In Asset Manager, you can configure the ServiceNow integration to have Asset Manager update ServiceNow at regular polling intervals, the cadence of which you set. This mechanism refreshes ServiceNow device details as often as you like, keeping them current.

Populating CMDB Data

A second use case uses a similar API exchange to answer the question, "What has Asset Manager discovered?" It shares with ServiceNow information about a device's profile, its status, and when it was first and last observed. It conveys timestamps and other network details to populate the Configuration Management Database (CMDB) within ServiceNow.

> ✅ **About CMDB**
>
> Configuration Management Database (CMDB) is an IT model for the efficient support of services and whose purpose is to organize and manage Configuration Items (CI).

Here's how it works:

1. Asset Manager queries ServiceNow at a regular interval and ingests CMDB data from ServiceNow, handling it as an external source.
2. Asset Manager compares data across the two systems.
3. Asset Manager pushes assets and attributes that are missing in ServiceNow to the ServiceNow server, which it populates the ServiceNow CMDB.
4. Asset Manager can push assets globally or by zone.

Asset Manager Dashboards within ServiceNow
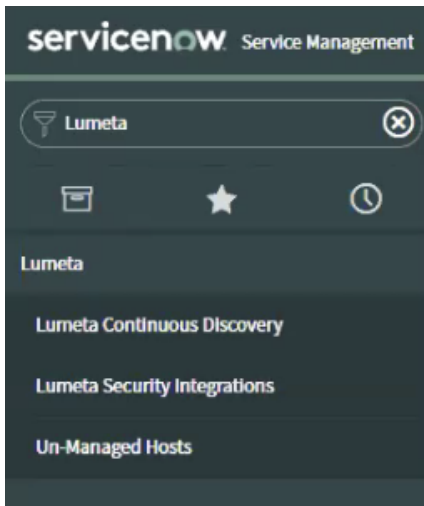
Asset Manager Continuous Discovery

From Asset Manager, each device profile, its status, first observed, and last observed timestamps, and other network details populating the CMDB database within ServiceNow.

All of the dashboards in ServiceNow can be personalized to display the columns of interest.