

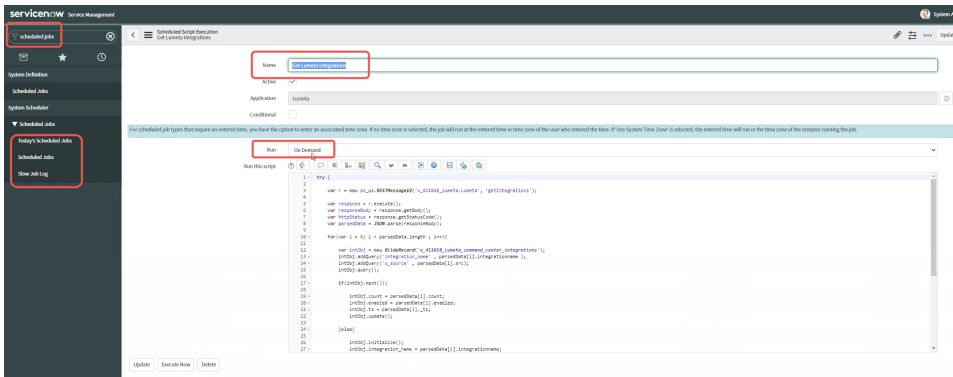
ServiceNow Integration Overview

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.

Lumeta Security Integrations					1 to 8 of 8	
All						
		Enabled	Integration Name	TS	Source(arc)	
<input type="checkbox"/>	①	true	Qualys	2020-07-07T12:52:54.367-04:00	qualys	
<input type="checkbox"/>	①	true	Tenable	2020-07-07T12:52:54.367-04:00	tenable	
<input type="checkbox"/>	①	false	Infoblox	2020-07-07T12:52:54.367-04:00	infoblox	
<input type="checkbox"/>	①	false	Redseal	2020-07-07T12:52:54.367-04:00	redseal	
<input type="checkbox"/>	①	true	Firemon	2020-07-07T12:52:54.367-04:00	firemon	
<input type="checkbox"/>	①	false	Carbonblack	2020-07-07T12:52:54.367-04:00	carbonblack	
<input type="checkbox"/>	①	true	Rapid7	2020-07-07T12:52:54.367-04:00	rapid7	
<input type="checkbox"/>	①	true	Epo	2020-07-07T12:52:54.367-04:00	epo	
<input type="checkbox"/>	Actions on selected rows					1 to 8 of 8

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?"

[illegible]

- Did Asset Manager identify a device lacking an agent such as McAfee or Carbon Black
- Did Asset Manager find a device that ServiceNow hasn't scanned? (Tenable, Qualys, Rapid7)?
- 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).

Incident INC0010004

Update Resolve Delete

Related Links

Repair SLAs

Task SLAs Un-Managed Hosts (2938)

Un-Managed Hosts New Search Lumeta Status Search

Incident = INC0010004

	Number	Device Type	DNS	SNOW Status	Lumeta Status	Integration-Type	IP	Mac	OS	TS
	UMH0012096	General Purpose		Un-Matched	Unresolved	Rapid7	10.101.17.16		Windows	2020-07-07T12:55:02.702-04:00
	UMH0012096	General Purpose		Un-Matched	Unresolved	Rapid7	10.64.8.5	00:22:41:32:45:d1	Unprofiled	2020-07-07T12:55:02.702-04:00
	UMH0012042	Unprofiled		Un-Matched	Unresolved	Rapid7	10.9.0.190		Unprofiled	2020-07-07T12:55:02.702-04:00
	UMH0012028	Appliance		Un-Matched	Unresolved	Rapid7	10.9.0.135		Linux	2020-07-07T12:55:02.702-04:00
	UMH0011195	General Purpose		Un-Matched	Unresolved	Rapid7	10.101.12.92		Windows	2020-07-07T12:55:02.702-04:00
	UMH0011111	General Purpose		Un-Matched	Unresolved	Rapid7	10.101.12.76		Windows	2020-07-07T12:55:02.702-04:00
	UMH0011227	General Purpose		Un-Matched	Unresolved	Rapid7	10.101.12.57		Windows	2020-07-07T12:55:02.702-04:00
	UMH0011243	General Purpose		Un-Matched	Unresolved	Rapid7	10.101.12.39		Windows	2020-07-07T12:55:02.702-04:00
	UMH0011259	General Purpose		Un-Matched	Unresolved	Rapid7	10.101.12.23		Windows	2020-07-07T12:55:02.702-04:00

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

Un-Managed Hosts New Search IP Search

All IP == 10.101.17.16

	Number	Device Type	DNS	Incident	SNOW Status	Lumeta Status	Integration-Type	IP	Mac	OS	TS
	UMH0004841	General Purpose		INC0010005	Un-Matched	Unresolved	Intable	10.101.17.16		Windows	2020-07-07T12:54:09.095-04:00
	UMH0010096	General Purpose		INC0010005	Resolved	Resolved	Rapid7	10.101.17.16		Windows	2020-07-07T12:55:02.702-04:00
	UMH0003042	General Purpose		INC0010003	Un-Matched	Unresolved	Dynat	10.101.17.16		Windows	2020-07-07T12:53:42.159-04:00
	UMH0007709	General Purpose		INC0010002	Un-Matched	Unresolved	Firemon	10.101.17.16		Windows	2020-07-07T12:54:35.720-04:00
	UMH0013624	General Purpose		INC0010001	Resolved	Resolved	Ego	10.101.17.16		Windows	2020-07-07T12:55:36.538-04:00

- 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.



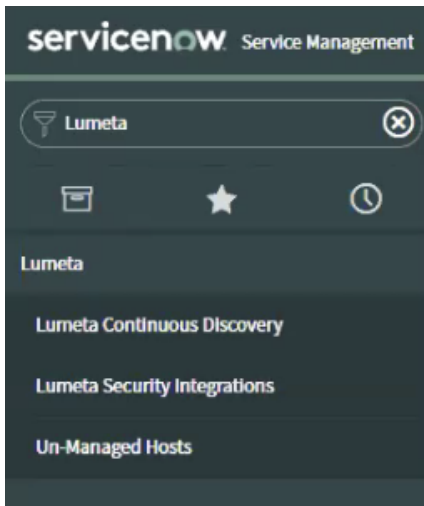
About CMDB

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:

- Asset Manager queries ServiceNow at a regular interval and ingests CMDB data from ServiceNow, handling it as an external source.
- Asset Manager compares data across the two systems.
- Asset Manager pushes assets and attributes that are missing in ServiceNow to the ServiceNow server, which it populates the ServiceNow CMDB.
- 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.

		Configuration Item	Device ID	Device Type	DNS Name	MAC	IP	First Observed	OS	Vendor	Version	Error
	①	true	--27119	27119			10.101.2.177	05/26/2020 09:26:30 AM				
	①	true	Windows-2000-30554	30554	General Purpose		10.101.9.69	05/26/2020 03:20:25 PM	Windows	Microsoft	2000	
	①	false	--33970	33970		00:90:27:01:00:0c		07/01/2020 04:00:01 AM				
	①	true	--32783	32783			192.168.112.248	06/17/2020 09:50:20 PM				

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

		Configuration Item	Device ID	Device Type	
	①	true	--27119	27119	
	①	true	Windows-2000-30554	30554	General Purpose
	①	false	--33970	33970	
	①	true	--32783	32783	
	①	true	Windows-2000-29742	29742	General Purpose
	①	true	Windows-NT-29211	29211	General Purpose
	①	true	Embedded JetDirect-30512	30512	Printer
	①	true	Windows-NT-30564	30564	General Purpose
	①	true	VMWare ESXi-26334	26334	General Purpose
	①	true	VMWare ESXi-26302	26302	General Purpose
	①	true	Linux-3.x-26223	26223	Appliance

Personalize List Columns

Available

Selected

☒ Wrap column text ☐ Compact rows ☐ Active row highlighting

☒ Modern cell coloring

☒ Enable list edit ☒ Double click to edit

Cancel

OK