DEPLOYMENT GUIDE

INFOBLOX UNIVERSAL ASSET INSIGHTS™ SERVICENOW INTEGRATION

DISCOVERY JOB CONFIGURATION AND CMDB RECONCILIATION

TABLE OF CONTENTS

INTRODUCTION

As organizations scale across hybrid and multi-cloud environments, maintaining an accurate **ServiceNow Configuration Management Database (CMDB)** becomes increasingly challenging. Manual updates, delayed discovery, and fragmented data sources often cause CMDB records to drift out of alignment with the actual state of the network. An up-to-date and authoritative asset inventory builds an accurate representation of what is located on customers' hybrid network and is essential not only for ensuring effective IT operations, but also for meeting governance, audit, and compliance requirements.

Infoblox Universal Asset Insights™ addresses this challenge by integrating with **ServiceNow** and providing a centralized solution that enables NetOps, CloudOps, and information technology service management (ITSM) teams to consolidate, normalize, and correlate asset data from a wide range of sources, including cloud APIs, on-premises discovery connectors, endpoint platforms, and third-party systems, like **Cisco Meraki**, **Juniper Mist**, and **CrowdStrike**. By ingesting and standardizing this data into a common asset database, **Universal Asset Insights** eliminates silos and data inconsistencies, offering a single source for unified assets across environments. This process enables continuous comparison between ServiceNow CMDB records and assets actively observed on the network, providing clear visibility into CMDB accuracy.

SERVICENOW INTEGRATION

Universal Asset Insights integrates with the ServiceNow CMDB using a secure, REST API–based connection configured and managed within the Infoblox Portal. This integration enables scheduled retrieval and validation of configuration item (CI) data from ServiceNow.

Once the connection is established, Universal Asset Insights retrieves CI records from the configured ServiceNow CMDB classes based on the selected discovery scope which is defined during the discovery job configuration.

For each CI, Universal Asset Insights collects key attributes including hostname, IP address, operating system and version, hardware and virtualization details, serial number, MAC address, location, region, and discovery timestamp details that go through a normalization and correlation process. This is a crucial step where asset records from ServiceNow are matched and reconciled with those discovered from cloud platforms (like **AWS**, **Azure**, and **Google Cloud**), on-premises environments, and other third-party integrations such as **Cisco Meraki**, **Juniper Mist**, **CrowdStrike**, and many other. The goal is to ensure consistency, eliminate duplicate entries, and enable cross-validation of ServiceNow records against real-world infrastructure. This process also helps uncover gaps, such as assets present in the environment but missing from the CMDB or discrepancies in ownership and configuration.

All correlated assets are unified and displayed in the Asset Inventory within the Network's Assets workspace under the **Asset Reconciliation** monitor of the Infoblox Portal, providing a consistent and validated view of assets across hybrid and multi-cloud environments.

Note: *The ServiceNow integration is* ***one-directional****. Universal Asset Insights retrieves and analyzes CMDB data from ServiceNow but does* ***not write back*** *or modify any records in the ServiceNow CMDB. This integration is read-only and does not introduce new data into ServiceNow, eliminating the risk of unintended CMDB changes.*

Type of Assets Discovered

During integration with ServiceNow, Universal Asset Insights discovers and processes CIs based on the configured discovery scope. The integration supports multiple CI classes across **Devices, Network Gear, Services, and related infrastructure domains**, enabling comprehensive asset visibility and reconciliation.

Currently, the supported CI classes include the following. This list will continue to expand as the integration matures, and updates will be reflected in this guide periodically.

cmdb_ci_computer – typically includes end-user and compute devices such as:

- Desktops and laptops
- Virtual machines (on-premises or cloud-based)
- Thin clients

cmdb_ci_server – includes server-class assets such as:

- Physical servers
- Virtual servers running on hypervisors

Operating system–specific server classes include:

- Linux servers
- Windows servers

Virtualization and hypervisor-related CI classes include:

- ESX hosts
- Virtual machine instances

Other device-related CI classes include:

- Printers

Network Gear Assets *(Always Included)*

Universal Asset Insights always discovers and ingests Network Gear–related CI classes. These assets are used for correlation and reconciliation and are currently **not configurable for exclusion**.

Supported CI classes include:

- **cmdb_ci_netgear**
    - cmdb_ci_ip_router
    - cmdb_ci_ip_switch
        - cmdb_ci_wap_network

    - cmdb_ci_ip_firewall
- cmdb_ci_network_adapter (often under hardware / network gear side)

Services and Infrastructure Services *(Always Included)*

Service-related CI classes are always included to ensure accurate correlation and dependency context.

Supported CI classes include:

- cmdb_ci_lb_service (load balancer/service classes)
- cmdb_ci_database
- cmdb_ci_security (security devices and equipment)

These CI classes are discovered, normalized, and correlated with assets observed through Infoblox discovery sources, enabling consistent asset classification and validation across hybrid and multi-cloud environments.

KEY CAPABILITIES

CMDB Accuracy Measurement and Visibility

Universal Asset Insights provides solution-grade visibility into ServiceNow CMDB accuracy by analyzing CMDB data against an authoritative, network-discovered asset inventory. By correlating ServiceNow CIs with assets discovered through a wide range of sources—including cloud APIs, on-premises discovery connectors, endpoint platforms, and third-party systems—the solution delivers an objective view of how closely the CMDB reflects actual infrastructure. Assets are automatically categorized to clearly identify alignment and gaps, enabling teams to quickly determine which records are accurate and missing.

Automated Asset Classification and Reporting

Universal Asset Insights continuously cross-validates ServiceNow CMDB records against the other discovered sources. During this process, assets are classified into three categories:

- Assets present in both ServiceNow CMDB and Infoblox discovery
- Assets present in ServiceNow CMDB but not currently observed on the network
- Assets actively observed on the network but missing from ServiceNow CMDB

This automated classification removes the need for manual reconciliation and provides a clear framework for prioritizing CMDB remediation efforts. Summary metrics provide at-a-glance visibility into CMDB data quality, while detailed reports identify specific assets requiring remediation and can be exported or scheduled for ongoing CMDB governance.

DISCOVERY JOB: PERMISSIONS REQUIRED AND CONFIGURATION ANALYSIS

PERMISSIONS REQUIRED FOR SERVICENOW

Before configuring the discovery job, please ensure that you have the appropriate access to the ServiceNow CMDB. This includes having valid API credentials or basic user credentials with **cmdb_read** permissions, which are required to allow the Infoblox Portal to successfully connect to ServiceNow and retrieve asset data. Without the correct access, the discovery job may fail to authenticate or fetch data, resulting in incomplete or inaccurate asset visibility.

The supported access method is as follows:

- Basic Authentication

If you are unsure whether the access method you are configuring has the necessary permissions, it is best to consult your ServiceNow administrator to confirm.

CONFIGURE SERVICENOW DISCOVERY JOB IN INFOBLOX PORTAL

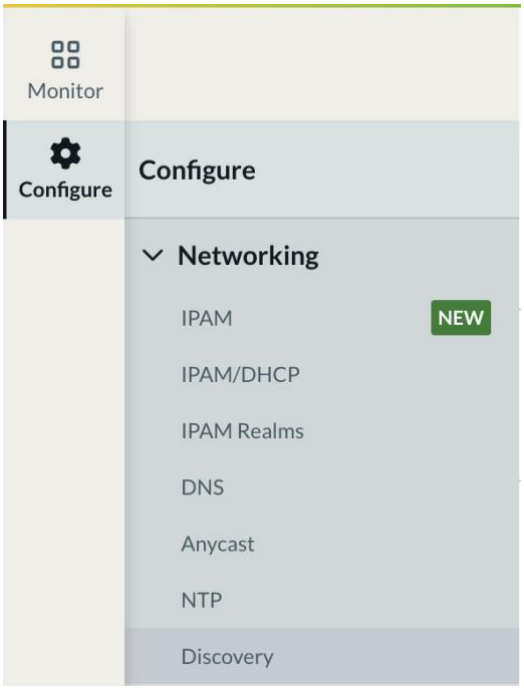
Configuring a discovery job to integrate Universal Asset Insights with ServiceNow involves setting up a secure connection. This setup is done through the Infoblox Portal on the **Configure -> Networking -> Discovery -> Integrations** page.

General

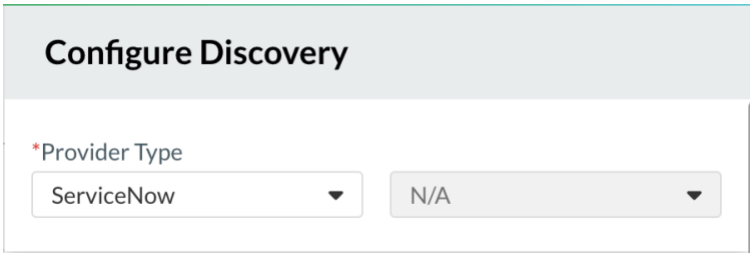
General Section

- Log in to the Infoblox Portal with an administrator account.

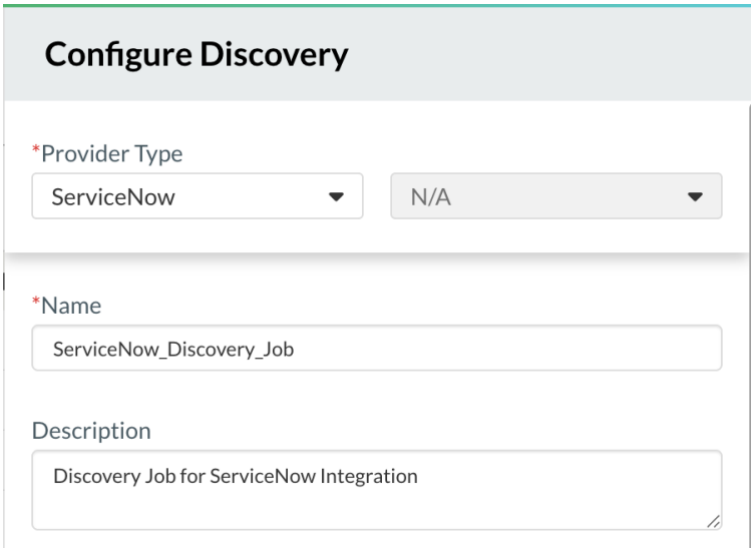
1. Navigate to **Configure -> Networking -> Discovery**.



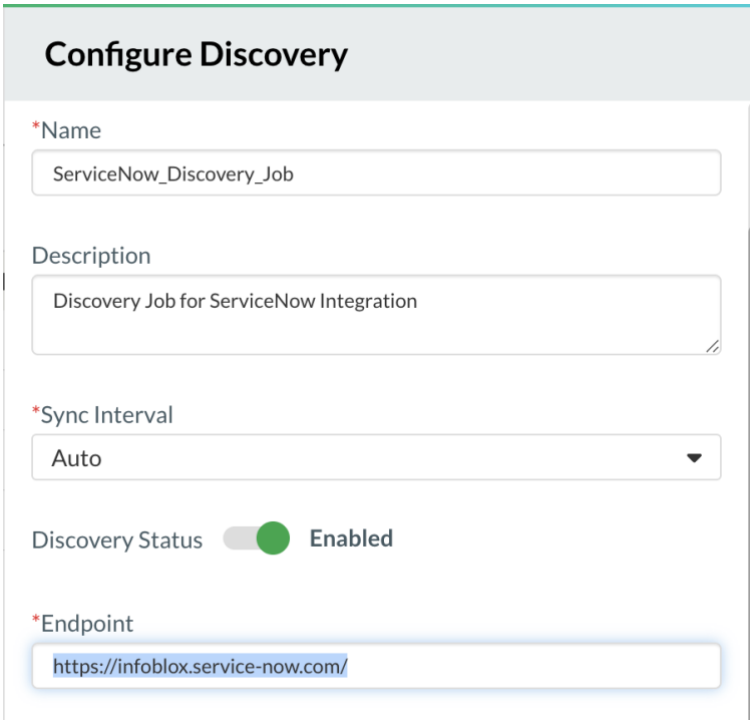
2. Click on **Integrations -> Configure Discovery ->** Select **ServiceNow** from the drop-down list.



3. **Name:** Assign a name to the discovery job.
4. **Description:** This is optional. Write an appropriate description for this job.



5. **Sync Interval:** Specifies how often the ServiceNow discovery job runs to synchronize and validate CMDB data; select **Auto** to allow the system to manage the schedule, or choose a fixed interval based on operational requirements.
    - **Discovery Status**: Leave this as **Enabled** (default).
    - **Endpoint:** Enter the base URL of your ServiceNow instance (for example, **https://<instance>.service-now.com**) that Universal Asset Insights will use to connect and retrieve CMDB data.

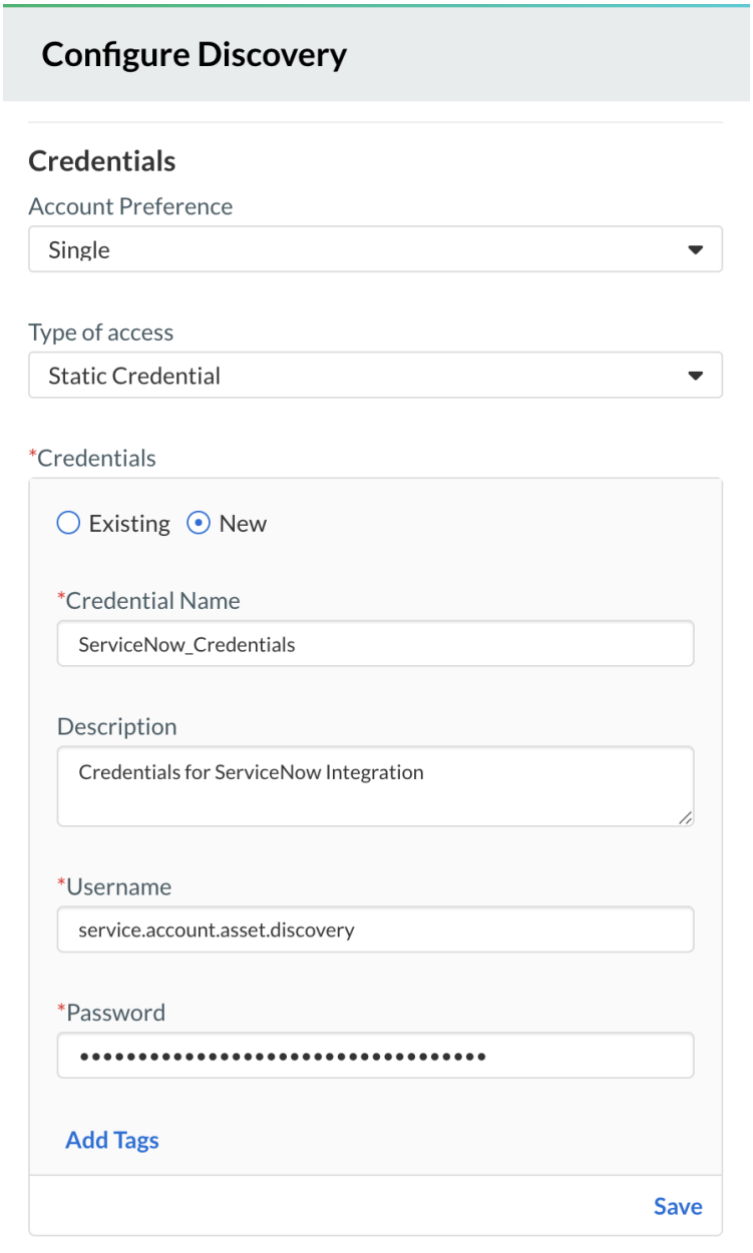


Credential Section

Use this section to select an existing ServiceNow credential or create a new one for the integration.

1. **Account Preference:** Select **Single** to use one ServiceNow account for authentication during the integration.
2. **Type of Access:** Select **Static Credential** as the authentication method; **only Static Credentials are supported** for this integration.
3. **Existing / New:** Select **New** to create a new ServiceNow credential, or **Existing** to reuse a previously configured credential.
4. **Credential Name:** Enter a descriptive name to identify the ServiceNow credential used for this integration.
5. **Description:** (Optional) Provide a brief description to indicate the purpose of the credential.
6. **Username:** Enter the ServiceNow service account username with permission to read CMDB data.
7. **Password:** Enter the password associated with the ServiceNow service account.

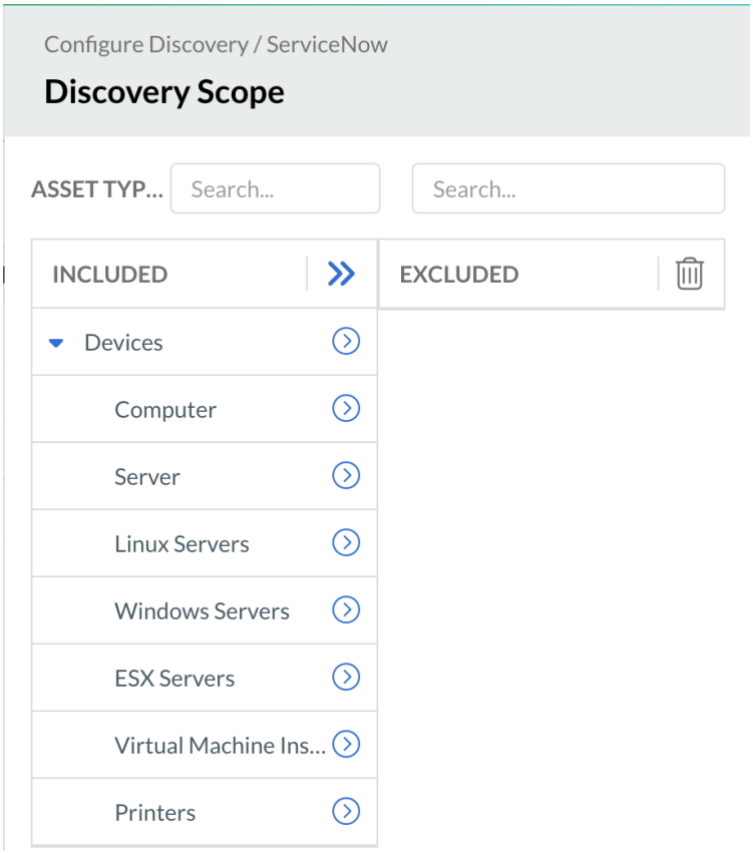
- **Tags:** (Optional) Add tags to help organize and manage credentials.
- Click **Save** to store the credential and return to the discovery job configuration.



Discovery Scope Section

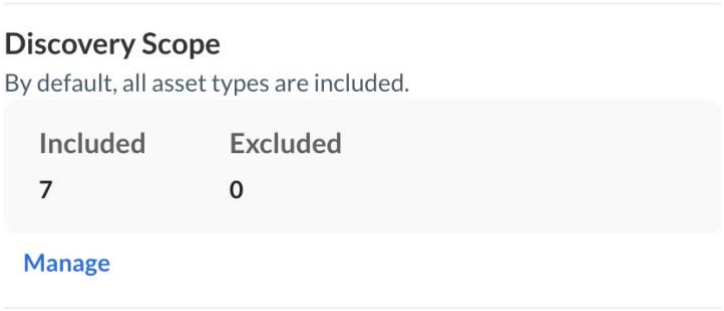
Use the Discovery Scope to control which ServiceNow CI classes are included or excluded from synchronization. **By default, all supported asset types are included.** You can refine the scope by selecting specific asset types under **Devices**—such as computers, servers, operating system-specific servers (Linux and Windows), ESX hosts, virtual machine instances, and printers—and moving them to the **Excluded** list as needed.

Note: Network Gear and Service-related CI classes are always included *as part of the current development and cannot be excluded from discovery at this time. Once sufficient data is available for analysis, additional controls may be introduced to allow exclusion of these CI classes.*



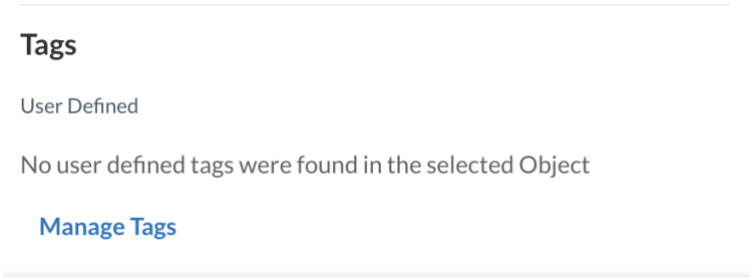
This allows you to tailor the integration to specific CI classes and limit data retrieval to assets relevant to your environment.

Here it displays the number of asset types included and excluded from synchronization; by default, all supported asset types are included, and you can click **Manage** to modify the scope.



Tags Section

Allows you to view and manage user-defined tags for the ServiceNow discovery job by adding, modifying, or removing tags to help with organization and easier management.

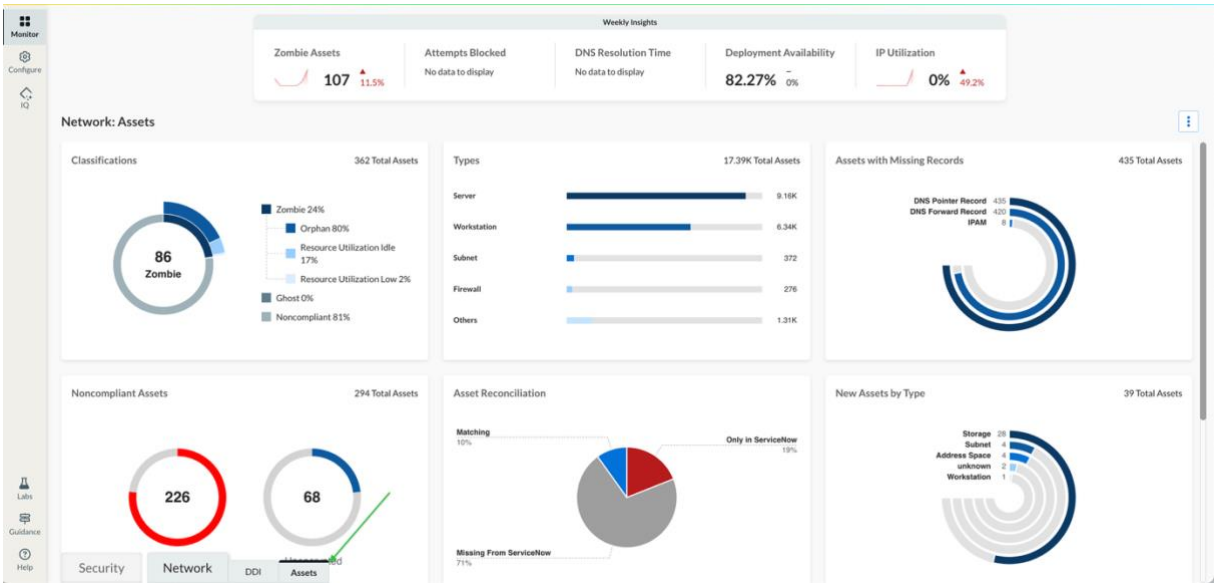


- Click **Save** to complete the discovery job configuration.

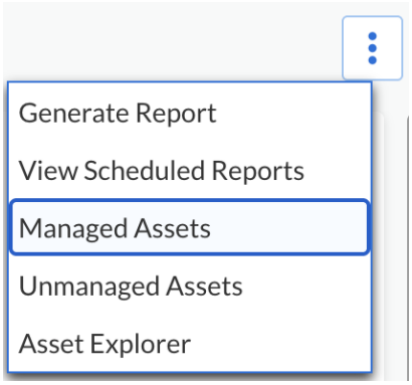
VIEW SERVICENOW ASSETS IN ASSET INVENTORY

After the ServiceNow discovery job has run successfully, use the Asset Inventory to explore which assets have been ingested from ServiceNow into Universal Asset Insights.

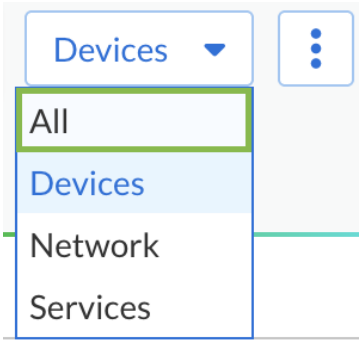
1. From Infoblox Portal, navigate to **Monitor -> Monitor** and select **Network -> Assets Workspace.**



2. In the Assets workspace, click the **ellipsis** menu and select **Managed Assets**.



- Ensure the **Devices** drop-down is set to **All** so that all ServiceNow derived assets are included in the view.

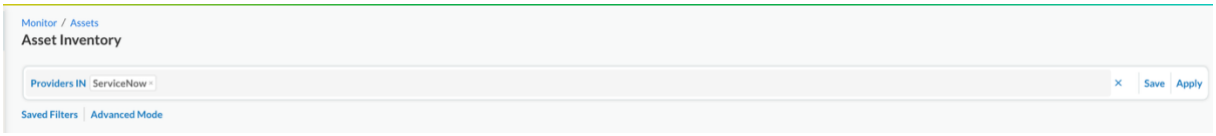


3. **Filter the inventory for ServiceNow discovered assets**

   I. Click the **Filter** button.

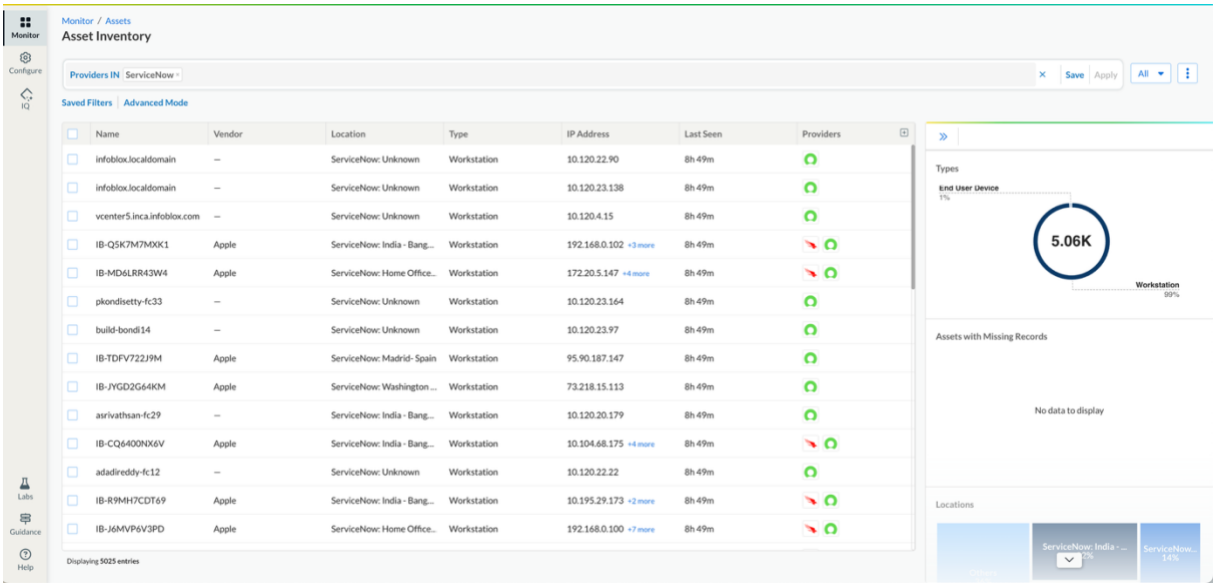
   II. In the filter panel, locate **Provider** and select **ServiceNow**.

   III. Apply any additional filters as needed (for example, by **Location**, **Region**, or **Category**) and then click **Apply**.



4. **Review the ServiceNow asset list**

   I. The Asset Inventory table now shows only assets discovered from **ServiceNow**.



   II. Optionally, customize the table by adding columns (using the + button) such as **Region**, **Category**, **OS**, or **Last Seen** to gain deeper insight into the imported CIs.

5. **Inspect an individual ServiceNow asset**

   - Click on any asset in the table to open its detailed view.
   - On the **Overview** tab, review key attributes such as vendor, model, serial number, IP address, MAC address, OS details, and discovery timestamps. If the same asset is discovered by multiple providers, all sources will be listed.

IB-Q5K7M7MXK1

OnPrem Device

Overview | Security | History

GENERAL DETAILS

Vendor
Apple

Cloud Account ID
N/A

Region
India - Bangalore

Location
servicenow:india - bangalore

Model
Apple MacBook Pro (16-inch, M2 Pro, 2023)

Serial Number
Q5K7M7MXK1

Operating System
Macos 15.5

IP Address
192.168.0.102
192.168.0.103
192.168.1.159
49.37.177.185

MAC Address
26:d0:da:fd:1d:64
5c:e9:1e:a9:44:9f
8e:e8:b1:6a:33:53
c6:c6:b8:d5:87:a6
+ 1 more

Type
Workstation

Registration Status
N/A

Managed
True

DISCOVERY INFORMATION

Discovery Source
Onprem:system

Providers

I. When Infoblox Threat Defense licenses are enabled, use the **Security** tab to review threats, policy violations, severities, actions, and linked events.

II. Use the **History** tab to see how the asset's state and associations have changed over time.

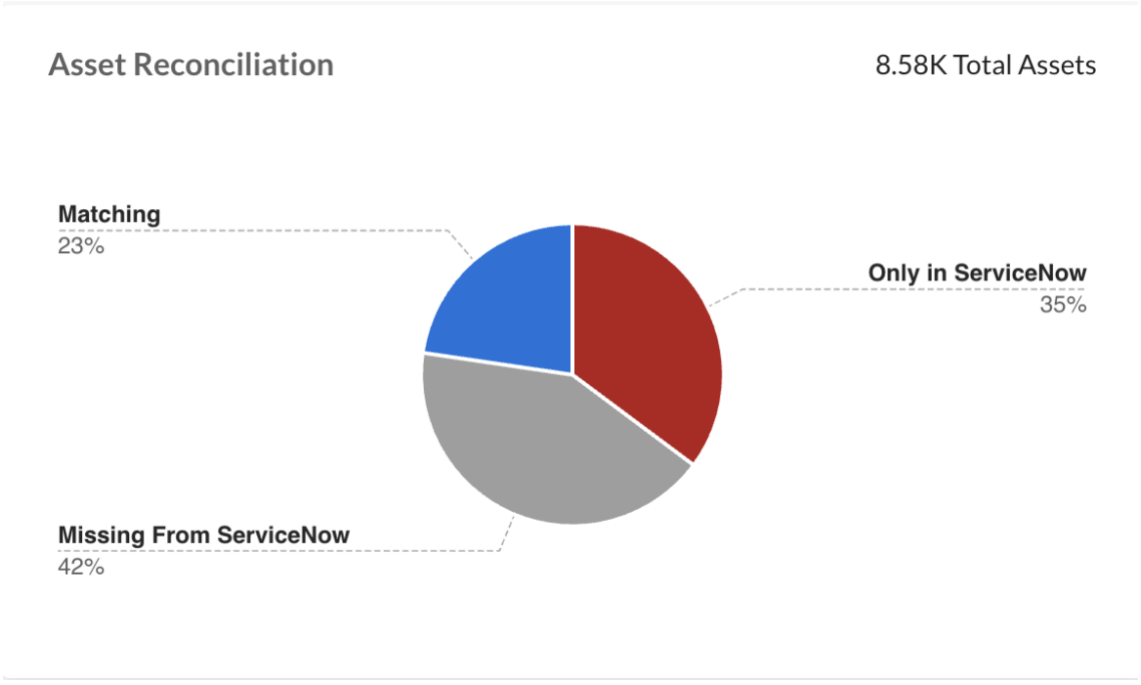
You can perform these steps at any time after the discovery job runs to validate that ServiceNow CMDB records are being ingested correctly and to spot-check specific CIs before working with the Asset Reconciliation monitor.

ASSET RECONCILIATION MONITOR

Once the discovery job is created and synchronization is successful, use the Asset Reconciliation Monitor to review CMDB validation results.

From Infoblox Portal, navigate to **Monitor -> Monitor** and select **Network -> Assets Workspace**. From the Assets workspace, access the **Asset Reconciliation Monitor** to review CMDB accuracy metrics and reconciliation results between ServiceNow CMDB records and network-discovered assets.

Note: *For accurate reconciliation results, one or more additional discovery sources must be enabled, such as Network Insight (NI) or DHCP logs for on-premises environments, cloud discovery for cloud-based assets, or third-party integrations such as CrowdStrike. If no additional discovery sources are configured, assets retrieved from ServiceNow will appear in the "**Only in ServiceNow**" category.*



Assets Present in Both ServiceNow CMDB and Infoblox Discovery

This metric represents assets for which a corresponding CI exists in ServiceNow CMDB, and which are also actively observed through Infoblox discovery sources such as cloud platforms (like AWS, Azure, and Google

Cloud), on-premises environments and other third-party integrations. These assets indicate accurate alignment between the CMDB and the actual network state and typically require no immediate remediation.

Assets Present in ServiceNow CMDB but Not Currently Observed on the Network
This metric identifies CIs that exist in ServiceNow CMDB but are not detected through Infoblox network discovery. These assets may represent decommissioned systems, powered-off devices, retired virtual machines, or outdated CMDB records. Reviewing this category helps identify stale entries that may need to be updated, validated, or removed from the CMDB.

Assets Actively Observed on the Network but Missing from ServiceNow CMDB
This metric highlights assets that are detected through Infoblox discovery but do not have corresponding CIs in ServiceNow CMDB. These assets may include newly deployed systems, short-lived cloud resources, or unmanaged devices. This category helps identify gaps in CMDB coverage and supports efforts to onboard missing assets into ServiceNow.

Available Actions

View and Export Assets in Asset Inventory

You can click on any widget or the total asset count in the Asset Reconciliation Monitor to view the corresponding assets in the Asset Inventory. From the Asset Inventory, detailed asset data can be exported to a CSV file for sharing with IT teams to support remediation activities or with management for reporting and executive summaries.

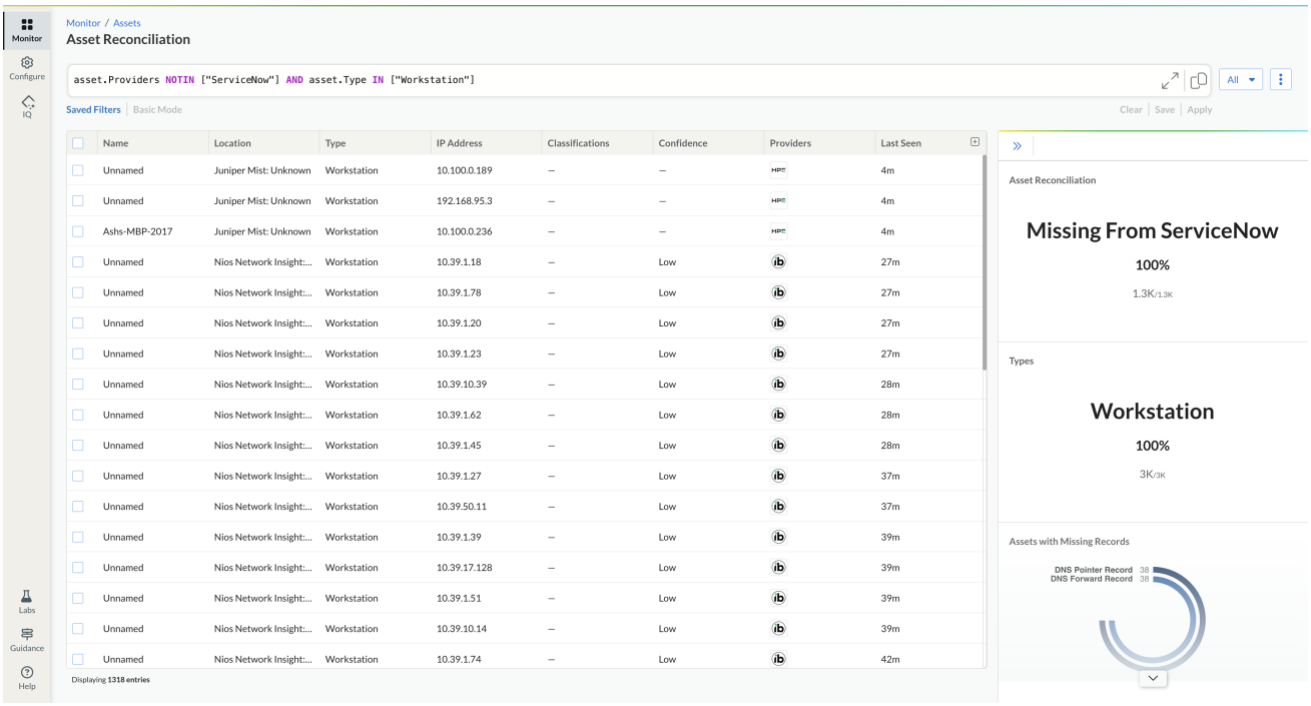
The following steps describe how to export assets from the Asset Inventory. These steps apply to **any monitor or filtered view** within the Asset Inventory.

1. Log in to the **Infoblox Portal**.
2. Navigate to **Monitor -> Monitor -> Network -> Assets Sub Workspace**.
3. From the **Asset Reconciliation Monitor**, click any widget or the total asset count to open the corresponding asset list.
4. In the **Asset Inventory** view, click the **ellipsis (⋯)** in the upper-right corner and select **Export All**.
5. Select the attributes you want to include in the export, then click **Export**.
6. A **CSV file** is downloaded to your local system and can be used for reporting, remediation workflows, or further analysis.

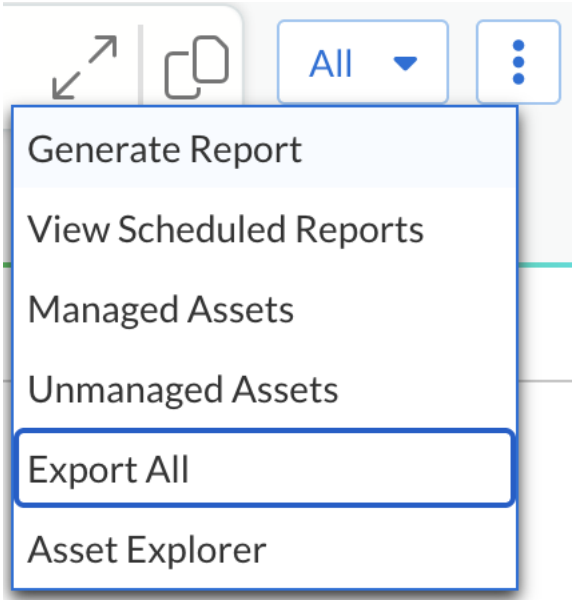
Customize Filters Before Exporting Assets

From the drill-down Asset Inventory view, you can further refine the asset list by modifying the query filters before exporting data. This allows you to narrow results to specific asset categories or attributes.

For example, if you want to export only assets that are **missing from ServiceNow** and are of type **Workstation**, you can update the query by adding a filter such as **Type = Workstation** while retaining the existing reconciliation filter. The Asset Inventory view updates dynamically based on the applied filters as shown in the screenshot below:



Once the desired filters are applied, use the **Export All** option to export only the filtered set of assets. This enables more targeted reporting and supports focused remediation efforts.



Generate Report

The **Generate Report** option allows you to create an on-demand report based on the current asset reconciliation view or applied filters. This report provides detailed visibility into asset categories, reconciliation status, and key attributes for each asset. Generated reports can be reviewed immediately or exported for offline analysis, audit preparation, or sharing with IT and operations teams. Use this option when an immediate snapshot of CMDB accuracy or asset discrepancies is required.

Schedule Report

The **Schedule Report** option enables automated generation of asset reconciliation reports at defined intervals. You can configure the report frequency and delivery method to ensure consistent visibility into CMDB data quality over time. Scheduled reports support ongoing CMDB governance by providing regular insights into asset alignment, newly identified discrepancies, and remediation progress without requiring manual report generation.

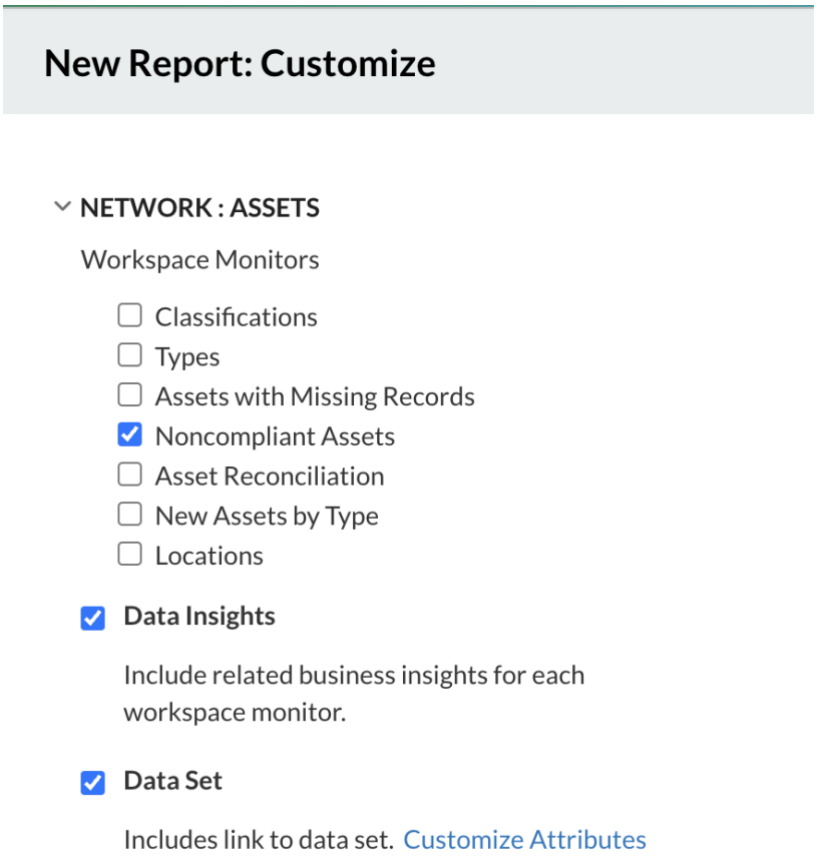
Generate or Schedule Asset Reconciliation Reports

Follow the steps below to generate or schedule Asset Reconciliation reports.

1. Log in to the **Infoblox Portal**.
2. Navigate to **Monitor -> Monitor -> Network -> Assets Workspace**.
3. From the **Asset Reconciliation Monitor**, click any widget or the total asset count to open the corresponding asset list.
4. In the **Asset Inventory** view, click the **ellipsis (⋯)** in the upper-right corner and select **Generate Report**.
5. Enter a **Report Name** and specify the **Recipients** to whom the report should be sent.

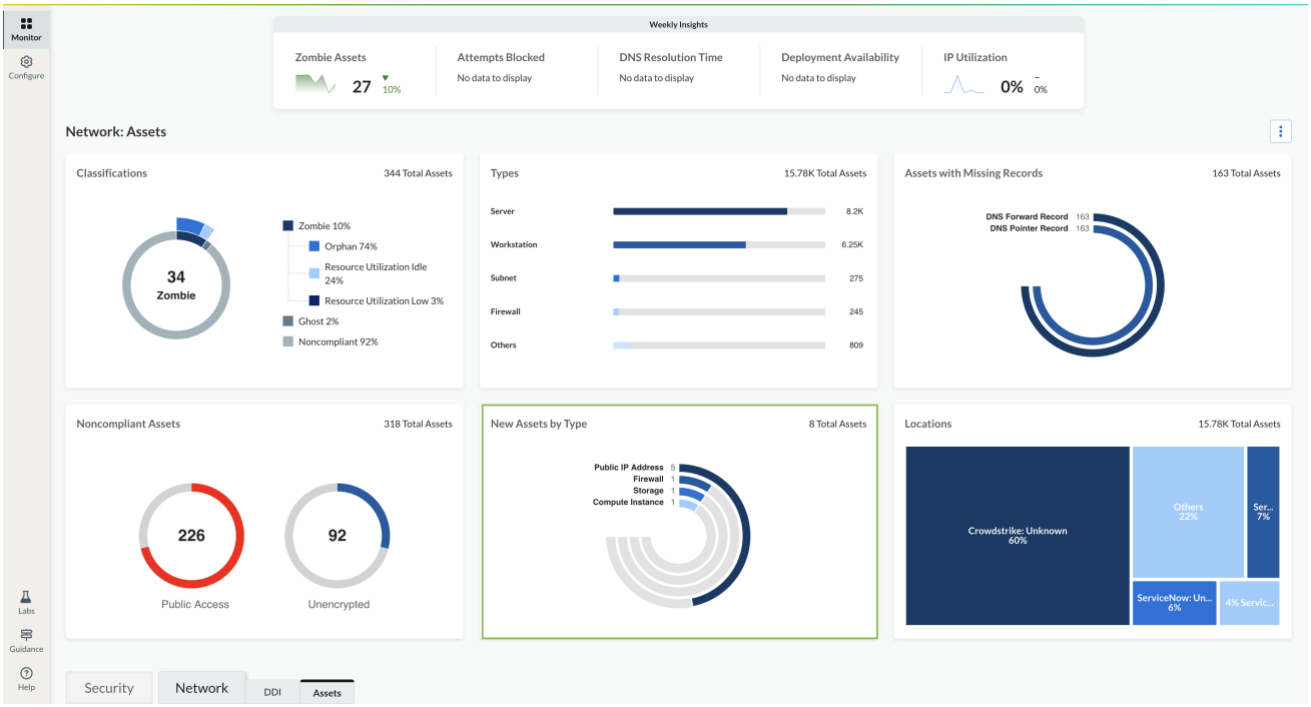
Note: *Email settings must be preconfigured for report delivery*.

6. By default, the **Assets Workspace** under the Network workspace is selected. To generate a report only for the **Asset Reconciliation Monitor**, click **Customize** and select **Asset Reconciliation Monitor**.



7. (Optional) Enable the **Data Set** option and click **Customize Attributes** to select the attributes to include in the report.
8. Click **Generate Now** to create the report immediately or select **Schedule** to configure automated report delivery.
9. For scheduled reports, select the **frequency**, **date**, and **time**, then click **Save**.
10. To view scheduled reports, click the **ellipsis (⋯)** and select **View Scheduled Reports**.
11. You can view **scheduled** and download **archived** reports from the menu by selecting the appropriate option.

Note: *The* ***Asset Reconciliation Monitor*** *is available only when the ServiceNow integration is configured. Without ServiceNow, the system displays the* ***New Assets by Type*** *monitor by default as shown below (in highlighted box).*


Monitor
Configure
Weekly Insights
Zombie Assets
27
10%
Attempts Blocked
No data to display
DNS Resolution Time
No data to display
Deployment Availability
No data to display
IP Utilization
0%
0%
Network: Assets
Classifications
344 Total Assets
34
Zombie
Zombie 10%
Orphan 74%
Resource Utilization Idle 24%
Resource Utilization Low 3%
Ghost 2%
Noncompliant 92%
Types
15.78K Total Assets
Server
8.2K
Workstation
6.25K
Subnet
275
Firewall
245
Others
809
Assets with Missing Records
163 Total Assets
DNS Forward Record 163
DNS Pointer Record 163
Noncompliant Assets
318 Total Assets
226
Public Access
92
Unencrypted
New Assets by Type
8 Total Assets
Public IP Address 5
Firewall 1
Storage 1
Compute Instance 1
Locations
15.78K Total Assets
Crowdstrike: Unknown
60%
Others
22%
Ser...
7%
ServiceNow: Un...
6%
4% Servic...
Labs
Guidance
Help
Security
Network
DDI
Assets

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business, providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste.
501 Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

Version: 20260118v1