DEPLOYMENT GUIDE

INFOBLOX UNIVERSAL ASSET INSIGHTS™ CROWDSTRIKE INTEGRATION

DISCOVERY JOB CONFIGURATION

TABLE OF CONTENT

INTRODUCTION

As organizations scale across hybrid and multi-cloud environments—spanning on-premises data centers, public cloud platforms like AWS, Azure and Google Cloud , as well as private cloud infrastructure—maintaining accurate and current asset visibility becomes more vital than ever. A reliable and authoritative asset inventory plays a key role not only in streamlining IT operations, but also in supporting governance, compliance and audit readiness.

Infoblox Universal Asset Insights™, a powerful product within the **Infoblox Universal DDI™ Product Suite**, automates the discovery and analysis of assets across major public clouds, on-premises networks and third-party solutions, such as CrowdStrike and ServiceNow, providing detailed and near-real-time visibility into network assets, giving organizations a unified, accurate view of all their IT assets. Universal Asset Insights addresses the above challenge by eliminating silos and data inconsistencies, offering a single source for unified assets across environments.

CrowdStrike is a leading cybersecurity platform that provides endpoint detection and response (EDR), threat intelligence and proactive threat hunting using the Falcon agent. It continuously monitors and records endpoint activity, enabling rapid threat detection, investigation and remediation with deep security insights.

Universal Asset Insights integrates with CrowdStrike in a hybrid, multi-cloud environment to deliver the best of both platforms. This integration consolidates asset discovery into a unified view, enriching asset data with near–real-time endpoint intelligence from CrowdStrike. As a result, organizations gain comprehensive visibility across cloud, on-premises and security domains—all through one centralized pane of glass.

CROWDSTRIKE INTEGRATION

Universal Asset Insights integrates seamlessly with CrowdStrike Falcon through a secure, API-based connection, easily configured within the Infoblox Cloud Services Portal. This integration enables Universal Asset Insights to retrieve near–real-time endpoint metadata from CrowdStrike, enriching its unified asset inventory with valuable security context. By integrating with CrowdStrike, Universal Asset Insights provides deeper visibility into endpoint behavior and status across hybrid and multi-cloud environments, helping IT and security teams make more informed operational decisions. The integration leverages CrowdStrike API endpoints to retrieve device identifiers and detailed device metadata, including device names, operating system types, IP addresses, MAC addresses and more as described in the **Type of Assets Discovered** section below.

This data is further passed through a normalization and consolidation process—where it is reconciled with asset data gathered from on-site environments, cloud platforms and other sources, including ServiceNow.

Furthermore, the assets are unified and presented under asset inventory, visible within the **Assets Workspace** under the **Monitor** section in the Infoblox Portal.

Type of Assets Discovered

Through its integration with CrowdStrike, Infoblox Universal Asset Insights discovers a wide range of devices, primarily focused on workstations, servers and domain controllers (DNS). This includes physical and virtual machines across on-premises infrastructure and public cloud environments, such as Azure, AWS and Google Cloud. For each discovered device, the integration shows a rich set of metadata, including device hostname, vendor, region, IP address, management address, model, serial number, MAC address and operating system. It also records discovery time stamps (first seen and last seen) and maintains a historical record of IP address assignments with associated date ranges, offering valuable lifecycle insights. Deeper security context is available when matching DNS and DHCP data, provided from Infoblox Universal DDI. This includes identifying the DHCP fingerprint of a device, verifying its DNS registration status and more.

KEY CAPABILITIES

Rich Unified Asset Inventory

CrowdStrike provides rich endpoint-level intelligence that complements infrastructure asset data. By integrating this data into the Universal Asset Insights platform, organizations can get greater visibility of device health, status and ownership, bringing endpoint awareness into the broader unified asset inventory where assets information is presented normalized and presented together from different sources, such as public cloud platforms, on-premises data centers and other third-party vendors, such as ServiceNow.

Cross-Validation of Assets Records

By correlating CrowdStrike telemetry with network and cloud assets, Infoblox Universal Asset Insights enables security and operations teams to identify endpoints that are vulnerable, non-compliant or operating outside of policy. This integration also helps uncover devices that are present in the environment but may not have CrowdStrike agents installed or may not be visible via other discovery sources, enabling security teams to take necessary actions.

With such rich data side by side in a single pane of glass, ITSM, SecOps and CloudOps teams can collaborate more effectively, ensuring accurate ownership attribution, prioritizing high-risk devices and improving the fidelity of compliance and vulnerability reports.

DISCOVERY JOB: PERMISSIONS REQUIRED AND CONFIGURATION ANALYSIS

PERMISSIONS REQUIRED FOR CROWDSTRIKE

Before configuring the discovery job, please ensure that you have appropriate access to CrowdStrike. This includes having the **Hosts Read** permission, which is required for the Infoblox Portal to successfully connect to CrowdStrike and retrieve device data. In addition to the Hosts Read permission, valid **API credentials** (**CLIENT_ID and CLIENT_SECRET**) are needed. These credentials are used to obtain an OAuth token, which is then used in subsequent API calls to fetch device data and device details. Without the correct access, the discovery job may fail to authenticate or retrieve data, leading to incomplete or inaccurate asset visibility.

CONFIGURE CROWDSTRIKE DISCOVERY JOB IN INFOBLOX PORTAL

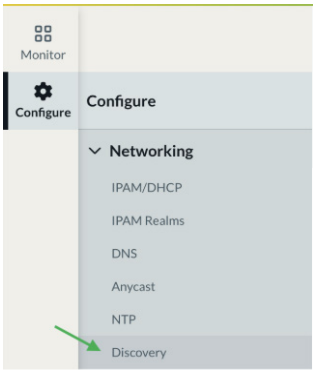
Configuring a discovery job to integrate Infoblox Universal Asset Insights with CrowdStrike involves setting up a secure connection. This setup is done through the Infoblox Portal on the **Configure -> Networking -> Discovery -> Third Party** page.

General

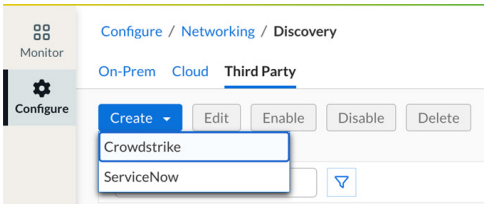
General Section

1. Log into the Infoblox Portal with an administrator account.

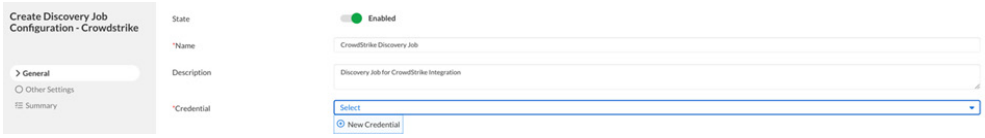
2. Navigate to **Configure -> Networking -> Discovery**.



3. Click on **Third Party -> Create -> CrowdStrike**.

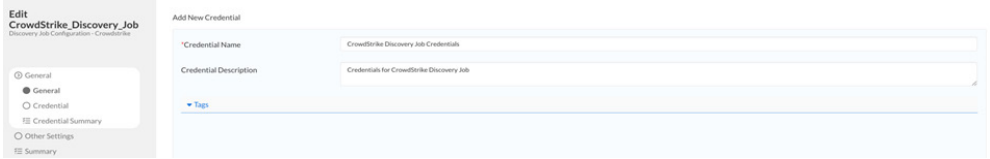


4. **State:** Change the discovery job state to **Enabled** (it is in **Disabled** state by default).
5. **Name:** Assign a name to the discovery job.
6. **Description:** This is optional. Write an appropriate description for this job.
7. **Credential:** Click on **Select** and from the drop-down, click on **New Credential**.

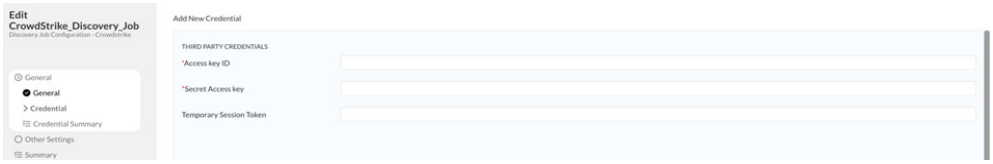


Credential Section

1. Provide the **Credential Name** and **Credential** Description.
2. Tags are optional. Click **Next**.



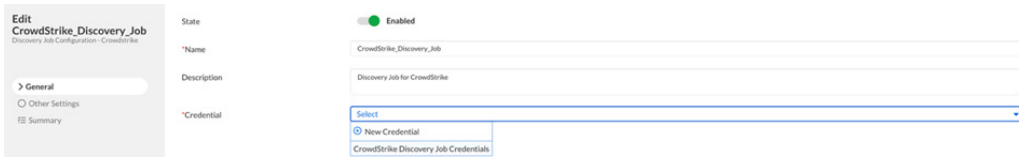
3. Under the **THIRD-PARTY CREDENTIALS** section, provide the **Access key ID, Secret Access ke**y and click **Next**. A **Temporary Session Token** is not mandatory so you can leave this blank.



Credential Summary Section

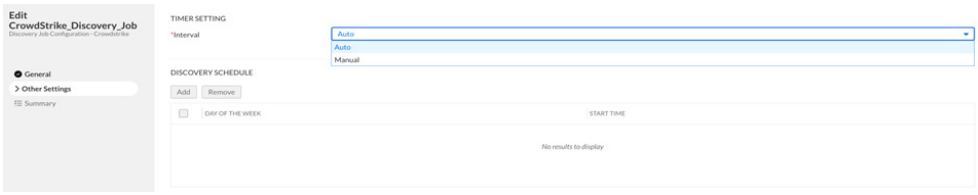
1. Review the credentials summary and click **Save**.

Note: This will return you to the **General** *section, where you can select the credentials you just created. Select the credentials and click* ***Next****.*

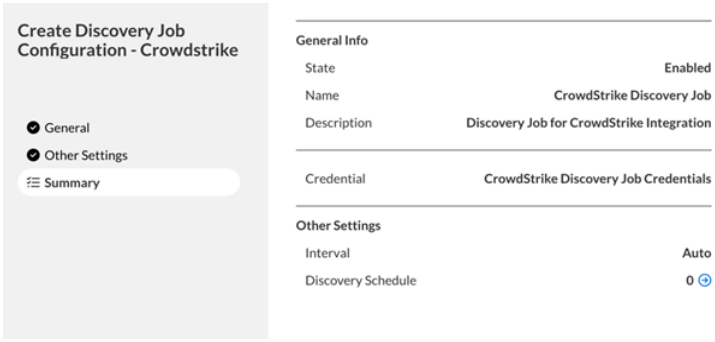


Other Settings

1. **TIMER SETTING -> Interval**: Select **Auto** or create a schedule from the **DISCOVERY SCHEDULE** section for a **Manual** interval.



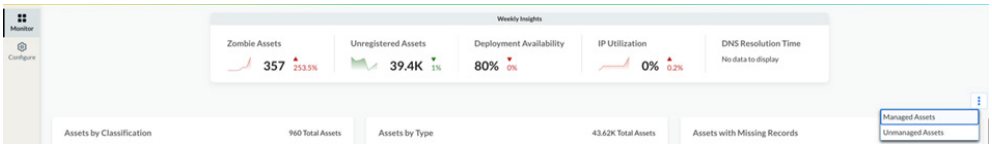
2. Click ***Next***. Review the summary and click **Save & Close**.



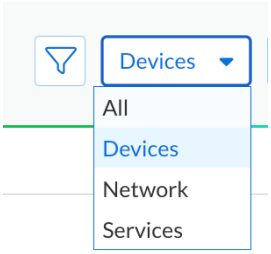
VIEW THE DISCOVERED DATA IN ASSET INVENTORY

Once the discovery job is created and sync is successful, follow these steps to view the discovered data under **Asset Inventory**.

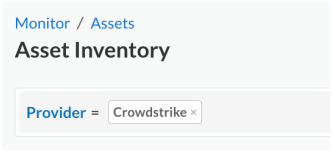
1. Click on **Monitor**, which will take you to the **Assets Workspace** by default.
2. Click on the ellipses and select **Managed Assets.**



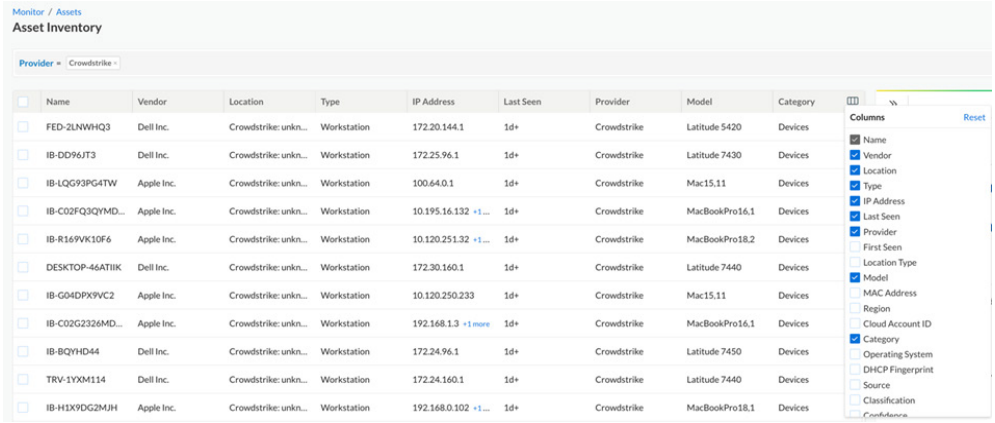
3. The **Devices** drop-down will open. Select **All**.



4. Click on the **Filter** button and select the **Provider** as **CrowdStrike**. Click **Apply**.



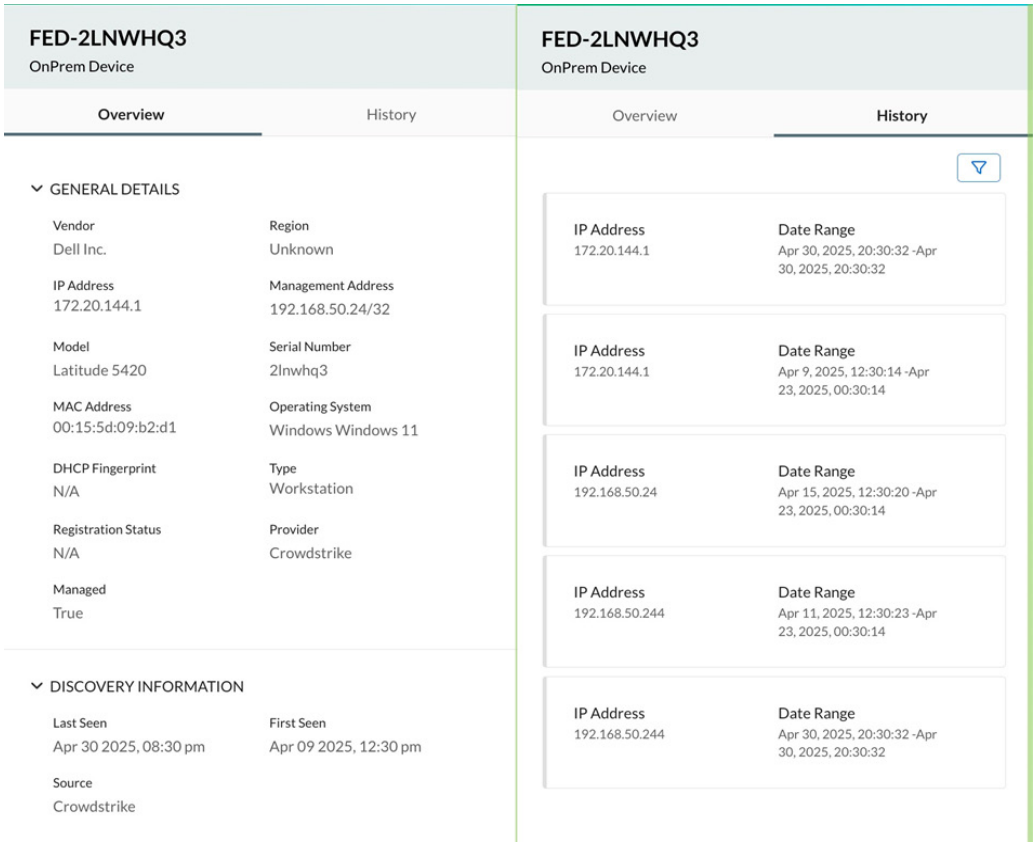
5. This will display the **Asset Inventory** for CrowdStrike assets. You can enhance the view by adding additional columns, like **Model** and **Category,** to gain deeper insights.



6. Click on any individual asset in the **Asset Inventory** to view detailed information collected during the discovery process.

The **Overview** tab displays key asset attributes such as vendor name, region, IP and management addresses, model and serial number, MAC address, operating system and discovery details—including first seen and last seen time stamps—along with other metadata retrieved from CrowdStrike.

The **History** tab provides a timeline of discovery events with each IP address it was associated with and the changes to it over time.



This information helps you gain a deeper understanding of the asset's characteristics and how it has changed over time within your environment.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20250516v1