

DEPLOYMENT GUIDE

INFOBLOX UNIVERSAL ASSET INSIGHTS™ INTEGRATION WITH CISCO CATALYST SD-WAN, JUNIPER MIST, VERSA NETWORKS AND ARUBA EDGECONNECT

INTEGRATION OVERVIEW, USE CASES,
AND DISCOVERY JOB CONFIGURATION

TABLE OF CONTENTS

INTRODUCTION	3
SOLUTION OVERVIEW	3
INTEGRATION OVERVIEWS & TYPE OF ASSETS DISCOVERED	4
Cisco Catalyst SD-WAN	4
Juniper Mist.....	4
Versa Networks.....	5
Aruba EdgeConnect.....	5
KEY CAPABILITIES	5
DISCOVERY JOBS: PERMISSIONS REQUIRED AND CONFIGURATION ANALYSIS	6
Cisco Catalyst SD-WAN.....	6
Permissions Required	6
Configure Cisco Catalyst SD-WAN Discovery Job	6
<i>General Section</i>	7
<i>Credentials Section</i>	8
<i>Destinations Section</i>	9
<i>Tags Section</i>	10
<i>Save the Discovery Job</i>	11
Juniper MIST.....	11
Permissions Required	11
Configure Juniper MIST Discovery Job	11
<i>General Section</i>	12
<i>Credentials Section</i>	13
<i>Discovery Scope Section</i>	14
<i>Ingestion Rules Section</i>	15
<i>Destinations Section</i>	15
<i>Tags Section</i>	16

<i>Save the Discovery Job</i>	16
Versa Networks	17
Permissions Required	17
Configure Versa Networks Discovery Job	17
<i>General Section</i>	18
<i>Credentials Section</i>	19
<i>Destinations Section</i>	20
<i>Tags Section</i>	21
<i>Save the Discovery Job</i>	21
Aruba EdgeConnect	22
Permissions Required	22
Configure Aruba EdgeConnect Discovery Job	22
<i>General Section</i>	23
<i>Credentials Section</i>	23
<i>Advanced Settings Section</i>	25
<i>Destinations Section</i>	25
<i>Tags Section</i>	26
<i>Save the Discovery Job</i>	26
VIEW THE DISCOVERED DATA IN THE INFOBLOX PORTAL.....	27
IPAM Data	27
Asset Inventory Data.....	28

INTRODUCTION

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, including network controllers and platforms such as **Cisco Catalyst SD-WAN**, **Juniper Mist**, **Versa Networks**, and **Aruba EdgeConnect**. This provides detailed and continuous visibility into network assets, giving organizations a unified, accurate view of all their IT assets.

This deployment guide describes how to operationalize the following **third-party integrations** with Universal Asset Insights:

- **Cisco Catalyst SD-WAN**
- **Juniper Mist**
- **Versa Networks**
- **Aruba EdgeConnect**

This guide is intended to complement the product UI and the individual configuration procedures for each integration. The focus here is on:

- The **integration model** and how Universal Asset Insights consume data from these platforms
- The **key capabilities and use cases** these integrations unlock for NetOps, SecOps, CloudOps, and IT service management (ITSM) teams
- The **types of assets discovered** and what they represent in the Infoblox inventory
- The **discovery job workflow**, required access/permissions, and how the resulting data is exposed in the Infoblox Portal

SOLUTION OVERVIEW

Universal Asset Insights ingests asset data from multiple sources and standardizes it into a common asset model. For the integrations covered in this guide, those sources include:

- **Cisco Catalyst SD-WAN:** Software-defined wide area network (SD-WAN) edge devices and controllers that provide L3 connectivity, along with the WAN-facing networks they terminate
- **Juniper Mist:** Cloud-managed site infrastructure (access points, switches, gateways) and the wired and wireless clients connected through that infrastructure
- **Versa Networks:** L3 SD-WAN appliances discovered from Versa Director (e.g., branch and hub routers) and their core device attributes as exposed via the appliances API
- **Aruba EdgeConnect:** L3 networking appliances, interfaces, subnets, and associated IP allocations across branch, data center, and cloud sites

The integration workflow is consistent with existing Universal Asset Insights integrations:

1. **Discovery jobs** are created in the Infoblox Portal for each provider.
2. Jobs use **secure API-based connections** (or provider-specific authentication) with read-only permissions to pull inventory and configuration metadata.
3. Retrieved data is **normalized and correlated** with other discovery sources (cloud, on-prem, configuration management database (CMDB), endpoint/security platforms).
4. Unified assets are exposed in the **Network -> Assets** sub-workspace and teams can **filter, export, and report** on these assets to improve operational efficiency, governance, and compliance.

INTEGRATION OVERVIEWS & TYPE OF ASSETS DISCOVERED

Cisco Catalyst SD-WAN

Cisco Catalyst SD-WAN delivers centralized, cloud-managed orchestration for WAN edge devices, secure connectivity, and application-aware routing across branches, data centers, and cloud locations.

Using the Universal Asset Insights integration with Cisco Catalyst SD-WAN, we discover Cisco SD-WAN edge devices and controllers (physical and virtual routers across branch, data center, and cloud environments, and the vManage and related control-plane nodes that manage the SD-WAN fabric), along with their WAN-facing network context (WAN interfaces and associated IP subnets, and the transport links used for branch-to-hub, branch-to-cloud, and data-center connectivity) and device metadata (device names, models and platform types, IP addresses and interface details, and role or usage such as branch edge, hub, or cloud gateway).

With these assets discovered and normalized in Universal Asset Insights, you can easily search for SD-WAN components in the Infoblox inventory, see which WAN edges exist and where they are deployed, understand how they interconnect, and visualize how SD-WAN prefixes and segments map into broader IP address management policies.

Juniper Mist

Juniper Mist is a cloud-based platform for managing wireless and wired access infrastructure with AI-driven operations. Using the Universal Asset Insights integration with Juniper Mist, we discover Mist-managed infrastructure devices (wireless access points, wired switches, and gateways or edge devices), their network context (sites, zones, site hierarchies, and associated wireless local-area networks (WLANs)/service set identifiers (SSIDs) and virtual local area networks (VLANs)), and the wired and wireless endpoint devices connected through that infrastructure, including client identity attributes such as hostname and operating system where available.

This provides an accurate, continuously updated view of campus and branch access infrastructure in the same inventory as your DDI (DNS, DHCP and IP address management), SD-WAN, and other third-party assets. You can see which APs, switches, and clients are active at each site, how they map to IP address space and VLANs, and how access layer health and utilization relate to the wider network.

Versa Networks

Versa Networks delivers a cloud-delivered SD-WAN and security platform that provides secure connectivity, application-aware routing, and unified policy enforcement across branches, data centers, and cloud locations.

Using the Universal Asset Insights integration with Versa Networks, we discover Versa SD-WAN appliances (L3 devices) from Versa Director (e.g., branch and hub routers) along with their device metadata (device name, device type or role such as branch or hub, and status indicators like online/offline or last-seen time) and network context (IP addresses and basic interface information for these appliances where available).

Aruba EdgeConnect

Aruba EdgeConnect is an SD-WAN platform that provides centralized, policy-based control over WAN connectivity across branches, and data centers. Using the Universal Asset Insights integration with Aruba EdgeConnect, we discover Aruba EdgeConnect appliances that provide L3 connectivity at branches, hubs, and data centers (e.g., branch/remote EdgeConnect appliances), along with the location where each appliance is deployed as shown in the Infoblox Portal.

With these assets discovered and normalized in Universal Asset Insights, you can search and filter for Aruba EdgeConnect appliances in the Infoblox inventory to see which devices exist at which locations, alongside Cisco Catalyst SD-WAN, Juniper Mist, and Versa assets.

KEY CAPABILITIES

Unified Asset Visibility Across SD-WAN, Campus Networks, and Physical Security

Enterprises often manage SD-WAN, wired, wireless, and physical security systems on separate platforms, each with its own inventory model and terminology. This makes it difficult to understand what devices are deployed at a site, which platforms own which assets and network segments, and whether assets appear in one system but not others, leading to slower day-to-day operations, more complex audits, and a higher risk of visibility gaps.

By integrating **Cisco Catalyst SD-WAN**, **Juniper Mist**, **Versa Networks**, and **Aruba EdgeConnect** into Universal Asset Insights, organizations gain a single, normalized asset inventory that spans WAN and campus domains (and can be viewed alongside data from physical security sources). Assets are consolidated and categorized by provider, type, and location, allowing teams to filter by platform while still viewing them in a common inventory. Asset Inventory clearly shows what exists at a location, which SD-WAN appliances, controllers, access devices, and clients are present, and which IP addresses they use (where available), resulting in faster operational awareness, fewer blind spots, and significantly less effort required to assemble cross-system views.

IPAM Synchronization for Accuracy and Compliance

SD-WAN overlays and campus networks frequently introduce new subnets and address spaces that are not consistently documented in core IP address management (IPAM). Devices move between sites or change connectivity dynamically, and new links or prefixes may never make it into formal IP plans, causing IP address records, subnet-utilization data, and network diagrams to drift out of sync with the actual environment.

By integrating **Cisco Catalyst SD-WAN**, **Juniper Mist**, **Versa Networks**, and **Aruba EdgeConnect** with Universal Asset Insights, subnet and IP information exposed by these platforms (e.g., WAN-facing networks on Cisco SD-WAN edges, VLANs and subnets from Mist-managed access networks, and interface-level IP data on Versa appliances) becomes visible in a centralized inventory and, where configured, can be synchronized into **Infoblox Universal IPAM**. At the same time, Aruba EdgeConnect appliances and their locations appear in the same correlated view, so teams can see how SD-WAN footprint and campus connectivity align with documented IP space even where EdgeConnect does not directly contribute new prefixes. Administrators gain end-to-end context into which networks and IP blocks are driven by SD-WAN and campus access policies, resulting in more reliable networks, consistent IP address allocation, and enhanced compliance readiness.

DISCOVERY JOBS: PERMISSIONS REQUIRED AND CONFIGURATION ANALYSIS

Cisco Catalyst SD-WAN

Permissions Required

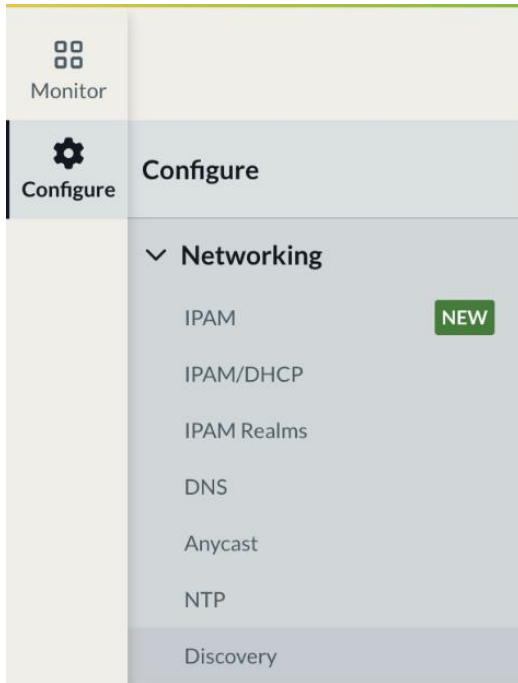
For the Cisco Catalyst SD-WAN integration, Universal Asset Insights requires a read-only API identity that can retrieve device inventory (SD-WAN edge devices, controllers, and gateways) and access interface and subnet information for WAN-facing connectivity.

In practice, this means creating an API user in Cisco vManage with inventory and configuration read permissions scoped to the devices and sites you will manage with Universal Asset Insights. Work with your Cisco SD-WAN administrators to create a dedicated service account/API user for Infoblox, assign minimum necessary read privileges, and confirm it can list the required devices and their WAN interfaces before using it in the discovery job. These credentials are then recorded in the Credentials section of the Cisco Catalyst SD-WAN discovery job configuration in the Infoblox Portal.

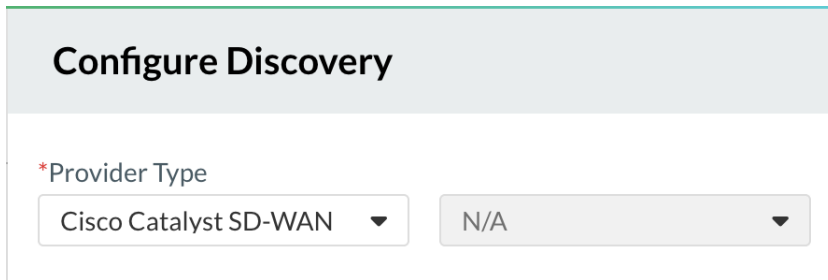
Configure Cisco Catalyst SD-WAN Discovery Job

Configuring a discovery job to integrate **Universal Asset Insights** with **Cisco Catalyst SD-WAN** involves setting up a secure connection to your SD-WAN controller (e.g., Cisco vManage). This setup is done through the Infoblox Portal on the **Configure -> Networking -> Discovery -> Integrations** page.

1. Log in to the Infoblox Portal with an administrator account.
2. Navigate to **Configure -> Networking -> Discovery**.



3. Click on **Integrations -> Configure Discovery -> Select Cisco Catalyst SD-WAN** from the drop-down list.



General Section

1. **Name:** Assign a name to the discovery job.
2. **Description:** This is optional. Write an appropriate description for this job.
1. **Sync Interval:** Specify how often the Cisco Catalyst SD-WAN discovery job runs to retrieve and synchronize SD-WAN asset data. Select **Auto** to allow the system to manage the schedule, or choose a fixed interval based on operational requirements.

Configure Discovery

*Provider Type

Cisco Catalyst SD-WAN ▼ N/A ▼

*Name

Cisco_SDWAN_Discovery_Job

Description

Discovery Job for Cisco Catalyst SD-WAN

*Sync Interval

Auto ▼

State Enabled

2. **Discovery State:** Leave this as **Enabled** (default).

Credentials Section

1. **Account Preference:** Select **Single** to use one Cisco SD-WAN account for authentication during the integration, or **Auto-Discover Multiple** to allow Universal Asset Insights to automatically discover and use multiple eligible Cisco SD-WAN accounts associated with the configured endpoint.
2. **Type of Access:** Select **Static Credential** as the authentication method; **only Static Credentials are supported** for this integration.
3. **Credentials:** Select **New** to create a new Cisco SD-WAN credential, or **Existing** to reuse a previously configured credential.
4. If you select **New**, provide the following:
 - a. **Credential Name:** Enter a descriptive name to identify the Cisco SD-WAN credential (e.g., Cisco SD-WAN – Read-Only API).
 - b. **Description:** (Optional) Add a short description indicating the purpose or scope of this credential.
 - c. **Username:** Enter the **Cisco SD-WAN (vManage) service account username** that has read-only access to device inventory, topology, and interface/tunnel/subnet information.
 - d. **Password:** Enter the password associated with the Cisco SD-WAN service account.

- e. **Tags:** (Optional) Add tags to help organize and manage credentials (e.g., prod, read-only).

Configure Discovery

Credentials

Account Preference

Single

Type of access

Static Credential

*Credentials

Existing New

*Credential Name

Cisco-SD-WAN-Creds

Description

Credentials for Cisco SD-WAN Integration

*Username

cisco.account.discovery

*Password

.....

[Add Tags](#)

[Save](#)

Endpoint

https://vmanage.example.com:8443

3. Click **Save** to store the credential and return to the discovery job configuration.
4. If you select **Existing** from the drop-down list, select the credentials that you have created already for Cisco SD-WAN in the Credentials section of the CSP portal.
5. **Endpoint:** Enter the base URL of your Cisco SD-WAN controller (e.g., https://<vmanage-fqdn>). This is the endpoint Universal Asset Insights will use to connect and retrieve SD-WAN inventory and topology data.

Destinations Section

6. **IPAM Discovery:** Enable this for Universal IP Address Management.
7. **Federated Realm: (Existing/New)** This option becomes available once the IPAM Discovery toggle is enabled. Select the **Destination Federated Realm** (e.g., **Default**) where you want the discovered networks to be created and managed. In most cases, a default realm is available for every tenant;

however, you can also create a new realm directly from this screen and point Cisco Catalyst SD-WAN-discovered networks to that realm instead.

8. **Tags:** (Optional) Add one or more tags to the Federated Realm to help classify, search, and report on IPAM destinations (e.g., environment, region, or business unit).

Destinations

IPAM Discovery Enabled

*Federated Realm

Existing New

Federated Realm

*Name

Description

[Add Tags](#)

[Save](#)

9. **Note:** *Federated Realm is a unified framework within Infoblox Universal DDI designed to streamline the planning and enforcement of IP address usage across multiple IPAM platforms, including on-premises and cloud environments, like AWS, Azure, and Google, and third-party networks. It provides a single hierarchical view of an enterprise's network, enabling administrators to manage IP address blocks, apply policies, and maintain consistency across diverse infrastructure sources. This model simplifies operations by abstracting backend complexities and offering a user-centric interface for managing IPAM. For additional details on IPAM Federation, refer to [Configure IPAM Federation](#).*

Tags Section

Use the Tags section to add, modify, or remove tags associated with the Cisco Catalyst SD-WAN discovery job. Tags can be used later for:

1. Grouping and searching discovery jobs.
10. Filtering or organizing jobs by environment (e.g., prod, staging, region-us-east).

Save the Discovery Job

After completing all the required sections:

1. Review the configuration for the Cisco Catalyst SD-WAN discovery job.
2. Click **Save** to complete the discovery job configuration.

Juniper MIST

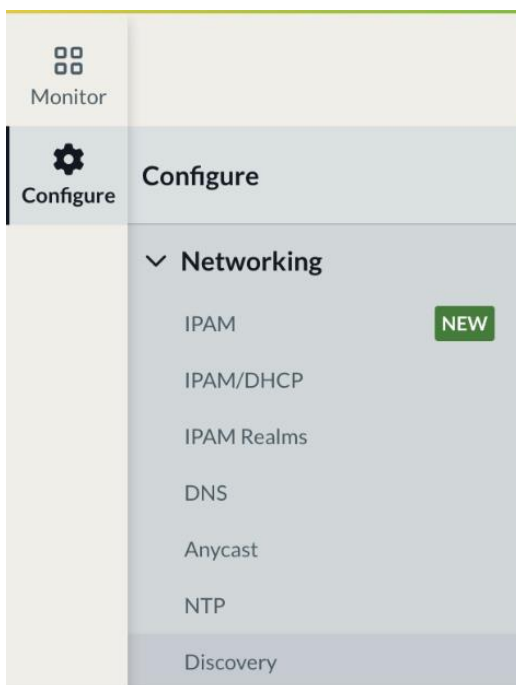
Permissions Required

For the Juniper Mist integration, Universal Asset Insights requires a read-only API token that can retrieve infrastructure inventory (wireless access points, wired switches, gateways), read site and zone definitions, and access WLAN/SSID, VLAN, and client information needed for asset correlation. Typically, this is a Mist API token with inventory and configuration read scopes for the Mist organizations you plan to manage, constrained to the relevant sites. Coordinate with your Juniper Mist administrators to create a dedicated API token for Infoblox, grant minimum-necessary read privileges, and verify that it can list devices, sites, WLANs/VLANs, and client records before you use it in the discovery job. The token is then stored in the **Credentials** section of the Juniper Mist discovery job configuration in the Infoblox Portal.

Configure Juniper MIST Discovery Job

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

1. Log in to the Infoblox Portal with an administrator account.
2. Navigate to **Configure -> Networking -> Discovery**.



3. Click on **Integrations** -> **Configure Discovery** -> Select **Juniper Mist** from the drop-down list.

Configure Discovery

*Provider Type

Juniper Mist N/A

General Section

1. **State:** Leave the discovery state as **Enabled** (default).
11. **Name:** Assign a name to the discovery job.
2. **Description:** This is optional. Write an appropriate description for this job.
3. **Sync Interval:** Specify how often the Cisco Catalyst SD-WAN discovery job runs to retrieve and synchronize SD-WAN asset data. Select **Auto** to allow the system to manage the schedule, or choose a fixed interval based on operational requirements.
12. **Provider URL:** Enter the base URL of the Juniper Mist cloud API endpoint you are using (e.g., <https://api.mist.com>). This is the endpoint Universal Asset Insights will use to connect and retrieve Juniper Mist inventory and topology data.

Configure Discovery

General

State Enabled

*Name
Mist_Discovery_Job

Description
Discovery Job for Juniper Mist

Sync Interval
Auto

*Provider URL
<https://api.mist.com>

Credentials Section

1. **Account Preference:** Select **Single**. Juniper Mist discovery supports only a single account for authentication per discovery job as of now.
2. **Type of Access:** Select **Static Credential** as the authentication method; **only Static Credentials are supported** for this integration as of now.
3. **Credentials:** Select **New** to create a new Juniper Mist credential, or **Existing** to reuse a previously configured credential.
4. If you select **New**, provide the following:
 - a. **Credential Name:** Enter a descriptive name to identify the Juniper Mist_credential.
 - b. **Description:** (Optional) Add a short description indicating the purpose or scope of this credential.
 - c. **API Key:** Enter the Juniper Mist API Key associated with an account that has read-only access to infrastructure devices (APs, switches, gateways), site information, and WLAN/VLAN and client data required for discovery.
 - d. **Tags:** (Optional) Add tags to help organize and manage credentials (e.g., prod, mist-credentials etc).
 - e. **Organization ID:** Enter the **Juniper Mist Organization ID** associated with this API token. This scopes discovery to that Mist organization. You can copy the Organization ID directly from the Juniper Mist portal.

Configure Discovery

Credentials

Account Preference
Single

Type of access
Static Credential

*Credentials

Existing New

Credentials

*Name
Mist_Creds

Description
Credentials for Juniper Mist Configuration

Authentication Type
 API Key

*API Key

[Add Tags](#)

[Save](#)

*Organization ID

13. Click **Save** to store the credential and return to the discovery job configuration.
14. If you select **Existing** in the drop-down list for Credentials, select the credential created in the Credentials section of the CSP portal for Juniper Mist vendor.

Discovery Scope Section

Use the **Discovery Scope** section to control which Juniper Mist organizations, sites, and asset types are included in synchronization.

1. By default, all supported Mist organization and their associated sites are included once you provide a valid Mist API token and Organization ID.
2. To refine the scope, click **Manage**.
3. Select what asset type from **Organization** and **Sites** you want Universal Asset Insights to discover.

Configure Discovery / Juniper Mist

Discovery Scope

ASSET TYP...

INCLUDED	EXCLUDED
Organization	
Devices	
Networks	
Sites	
Sites	
Devices	
Wireless Clients	
Wired Clients	
Networks	

4. Click **Save** once asset types are include/excluded in the discovery. This allows you to limit discovery to the Mist-managed environments and asset classes that are relevant to your deployment, reducing noise while preserving complete visibility where it matters.

Ingestion Rules Section

Use the Ingestion Rules section to control which SSIDs from Juniper Mist are included in discovery. By default, all SSIDs in the selected organizations/sites are eligible for ingestion. To refine this, click **Add Rules**.

15. Include only specific SSIDs that you want Universal Asset Insights to ingest (e.g., production or corporate SSIDs), or
 1. Exclude SSIDs that should be ignored (e.g., guest, lab, or temporary SSIDs).
 2. Click **Save**. These rules help you limit discovery to business-relevant wireless networks and avoid clutter from non-critical or transient SSIDs.

Destinations Section

16. **IPAM Discovery:** Enable this to allow Juniper Mist-managed subnets and networks to be discovered into Universal IP Address Management.
17. **Federated Realm: (Existing/New)** This option becomes available once the IPAM Discovery toggle is enabled. Select the destination Federated Realm (e.g., Default) where you want the discovered Mist networks to be created and managed. In most cases, a default realm is available for every tenant; however, you can also create a new realm directly from this screen and point Juniper Mist-discovered networks to that realm instead.

18. **Tags:** (Optional) When creating a new Federated Realm, add one or more tags to the Federated Realm to help classify, search, and report on IPAM destinations (e.g., environment, region, or business unit).

Destinations

IPAM Discovery Enabled

*Federated Realm

Existing New

Federated Realm

*Name

Description

[Add Tags](#)

[Save](#)

19. **Note:** Federated Realm is a unified framework within Infoblox Universal DDI designed to streamline the planning and enforcement of IP address usage across multiple IPAM platforms, including on-premises and cloud environments, like AWS, Azure, and Google, and third-party networks. It provides a single hierarchical view of an enterprise's network, enabling administrators to manage IP address blocks, apply policies, and maintain consistency across diverse infrastructure sources. This model simplifies operations by abstracting backend complexities and offering a user-centric interface for managing IPAM. For additional details on IPAM Federation, refer to [Configure IPAM Federation](#).

Tags Section

Use the Tags section to add, modify, or remove tags associated with the Juniper Mist discovery job. Tags can be used later for:

1. Grouping and searching discovery jobs.
2. Filtering or organizing jobs by environment (e.g., prod, staging, region-us-east).

Save the Discovery Job

After completing all the required sections:

1. Review the configuration for the Juniper Mist discovery job.
20. Click **Save** to complete the discovery job configuration.

Versa Networks

Permissions Required

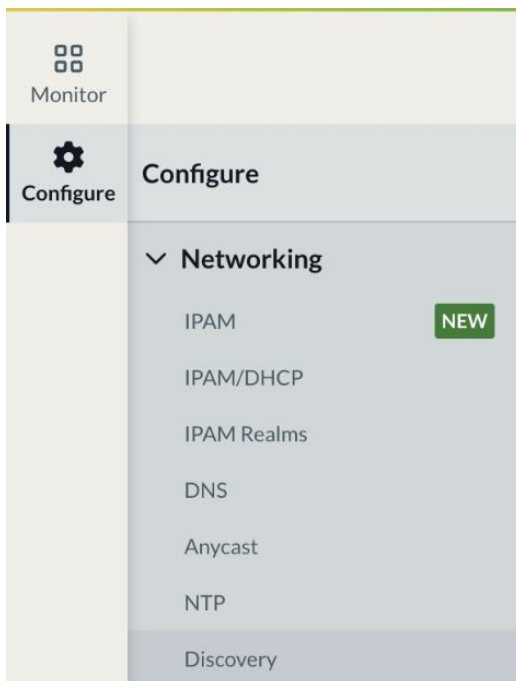
For the Versa Networks integration, Universal Asset Insights requires a read-only API identity that can retrieve device inventory for Versa SD-WAN appliances (L3 devices) from Versa Director and, where available, access interface and IP address information for those appliances.

In practice, this typically means creating an API user in Versa Director with inventory and configuration read scopes for the appliances you plan to manage with Universal Asset Insights. Work with your Versa Networks administrators to create a dedicated integration identity for Infoblox, assign minimum-necessary read privileges, and confirm that it can list the relevant appliances and their basic interface/IP information before using it in the discovery job. These credentials are then recorded in the **Credentials** section of the Versa discovery job configuration in the Infoblox Portal.

Configure Versa Networks Discovery Job

Configuring a discovery job to integrate Universal Asset Insights with Versa Networks involves setting up a secure connection to the Versa management plane (e.g., Versa Director or a cloud hosted- controller). This setup is done through the Infoblox Portal on the **Configure -> Networking -> Discovery -> Integrations** page.

1. Log in to the Infoblox Portal with an administrator account.
2. Navigate to **Configure -> Networking -> Discovery**.



21. Click **Integrations -> Configure Discovery**, then select **Versa Networks** from the drop-down list.

Configure Discovery

*Provider Type

Versa Networks

N/A

General Section

1. **Name:** Assign a name to the discovery job.
2. **Description:** This is optional. Write an appropriate description for this job.
3. **Sync Interval:** Specify how often the Versa Networks discovery job runs to retrieve and synchronize asset data. Select **Auto** to allow the system to manage the schedule, or choose a fixed interval based on operational requirements.
4. **Discovery Status:** Leave this as **Enabled** (default) unless you want to create the job in a disabled state.
22. **Endpoint:** Enter the base URL of your Versa Networks management plane (e.g., `https://<versa-director-fqdn>:<port>`). This is the endpoint that Universal Asset Insights uses to connect to Versa and retrieve SD-WAN inventory and topology data.

*Provider Type

Versa Networks

N/A

*Name

Versa_Networks_Job

Description

Enter job description

*Sync Interval

Auto

Discovery Status Enabled

*Endpoint

https://cloud-demo.versa-networks.com:9182

Credentials Section

1. **Account Preference:** Select **Single**. Versa discovery configuration uses a single account per discovery job.
2. **Type of Access:** Select **Static Credential** as the authentication method; **only Static Credentials are supported** for this integration as of now.
3. **Credentials:** Select **New** to create a new Versa credential, or **Existing** to reuse a previously configured credential.
4. If you select **New**, provide the following:
 - a. **Credential Name:** Enter a descriptive name to identify the Versa_credential.
 - b. **Description:** (Optional) Add a short description indicating the purpose or scope of this credential.
 - c. **Username:** Enter the **Versa** username associated with an account that has read-only access to device inventory, topology, and interface/tunnel/subnet information.
 - d. **Password:** Enter the password associated with the Versa user account.
 - e. **Tags:** (Optional) Add tags to help organize and manage credentials (e.g., prod, versa-credentials etc).
 - f. **Organization ID:** Enter the **Versa Organization ID** associated with this user account. This scopes discovery to that Versa organization.

Configure Discovery

Credentials

Account Preference
Single

Type of access
Static Credential

*Credentials

Existing New

*Credential Name
Versa_Network_Credentials

Description
Credentials for Versa Networks

*Username
versa-discovery-account

*Password
.....

Add Tags

Save

*Organization ID

23. Click **Save** to store the credential and return to the discovery job configuration.

Destinations Section

24. **IPAM Discovery:** Enable this if you want Versa networks and IPs to be written into Universal IPAM.

25. **Federated Realm: (Existing/New)** This option becomes available once the IPAM Discovery toggle is enabled. Select the destination Federated Realm (e.g., Default) where you want the discovered Versa networks to be created and managed. In most cases, a default realm is available for every tenant; however, you can also create a new realm directly from this screen and point Versa discovered networks to that realm instead.

26. **Tags: (Optional)** Add one or more tags to the Federated Realm to help classify, search, and report on IPAM destinations (e.g., environment, region, or business unit).

Note: *Federated Realm is a unified framework within Infoblox Universal DDI designed to streamline the planning and enforcement of IP address usage across multiple IPAM platforms, including on-premises and cloud environments like AWS, Azure, and Google, and third-party networks. It provides a single hierarchical view of an enterprise's network, enabling administrators to manage IP address blocks, apply policies, and maintain consistency across diverse infrastructure sources. This model simplifies operations by abstracting backend complexities and offering a user-centric interface for managing IPAM. For additional details on IPAM Federation, refer to [Configure IPAM Federation](#).*

Destinations

IPAM Discovery Enabled

*Federated Realm

Existing New

Federated Realm

*Name

Description

[Add Tags](#)

[Save](#)

Tags Section

Use the **Tags** section to add, modify, or remove tags associated with the **Versa** discovery job. Tags can be used later for:

1. Grouping and searching discovery jobs.
2. Filtering or organizing jobs by environment (e.g., prod, staging, region-us-east).

Save the Discovery Job

After completing all the required sections:

1. Review the configuration for the Versa discovery job.
2. Click **Save** to complete the discovery job configuration.

Aruba EdgeConnect

Permissions Required

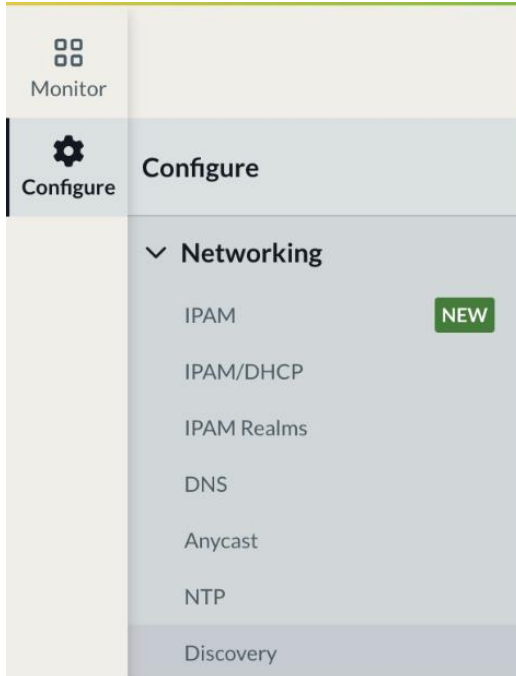
For the Aruba EdgeConnect integration, Universal Asset Insights requires a read-only API identity that can retrieve Aruba EdgeConnect appliance inventory and their associated location information from the Aruba Orchestrator management plane. In practice, this typically means creating an Orchestrator user or API client with inventory and configuration read permissions for the appliances you plan to manage with Universal Asset Insights.

Work with your Aruba EdgeConnect administrators to create a dedicated integration identity for Infoblox, assign minimum-necessary read privileges, and confirm that it can list the relevant appliances and their locations before using it in the discovery job. These credentials are then recorded in the Credentials section of the HPE Aruba EdgeConnect discovery job configuration in the Infoblox Portal.

Configure Aruba EdgeConnect Discovery Job

Configuring a discovery job to integrate Universal Asset Insights with Aruba EdgeConnect involves setting up a secure connection to the EdgeConnect/Orchestrator management plane. This setup is done through the Infoblox Portal on the **Configure -> Networking -> Discovery -> Integrations** page, following the same pattern used for Cisco Catalyst SD-WAN and Versa Networks.

1. Log in to the Infoblox Portal with an administrator account.
2. Navigate to **Configure -> Networking -> Discovery**.



3. Click **Integrations -> Configure Discovery**, then select **Aruba EdgeConnect** from the drop-down list.

Configure Discovery

*Provider Type

Aruba EdgeConnect ▼ N/A ▼

General Section

1. **Name:** Assign a name to the discovery job.
2. **Description:** This is optional. Write an appropriate description for this job.
3. **Sync Interval:** Specify how often the Aruba EdgeConnect discovery job runs to retrieve and synchronize SD-WAN asset data. Select **Auto** to allow the system to manage the schedule, or choose a fixed interval based on operational requirements.
4. **Discovery Status:** Leave this as **Enabled** (default) unless you want to create the job in a disabled state.

Configure Discovery

*Provider Type

Aruba EdgeConnect ▼ N/A ▼

*Name

Enter job name

Description

Enter job description

*Sync Interval

Auto ▼

State Enabled

Credentials Section

1. **Account Preference:** Select **Single** to use one HPE Aruba EdgeConnect account for authentication during the integration, or **Auto-Discover Multiple** to allow Universal Asset Insights to automatically discover and use multiple eligible HPE Aruba EdgeConnect accounts associated with the configured endpoint.
2. **Type of Access:** Select **Static Credential** as the authentication method; **only Static Credentials are supported** for this integration as of now.

3. **Credentials:** Select **New** to create a new Aruba EdgeConnect credential, or **Existing** to reuse a previously configured credential.
4. If you select **New**, provide the following:
 - a. **Credential Name:** Enter a name for the Aruba EdgeConnect credential.
 - b. **Description:** (Optional) Add a short description indicating the purpose or scope of this credential.
 - c. **Username:** Enter the **Aruba EdgeConnect** username associated with an account that has read-only access to device inventory, topology, and interface/tunnel/subnet information.
 - d. **Password:** Enter the password associated with the Aruba EdgeConnect user account.
 - e. **Tags:** (Optional) Add tags to help organize and manage credentials (e.g., prod, EdgeConnect-credentials etc).

Configure Discovery

Credentials

Account Preference

Single

Type of access

Static Credential

*Credentials

Existing New

*Credential Name

Enter credential name

Description

Enter credential description

*Username

Enter Orchestrator username

*Password

Enter Orchestrator password

[Add Tags](#)

Save

27. Click **Save** to store the credential and return to the discovery job configuration.
28. **Orchestrator URL:** In the Orchestrator URL field, enter the URL of your HPE Aruba EdgeConnect Orchestrator instance (e.g., <https://orchestrator.example.com>). This endpoint must be reachable from the Infoblox SaaS platform and should match the certificate presented by Orchestrator in production environments.

Advanced Settings Section

29. **TLS settings – Skip TLS Verification:** Use this control to manage TLS certificate verification for the connection to Orchestrator.
30. Insights validates the Orchestrator server certificate (hostname, trust chain, and expiry) before establishing the connection.
31. **Lab/Testing Only:** Temporarily enable *Skip TLS Verification* **only** for non-production environments (e.g., lab Orchestrator instances using self-signed certificates). This bypasses certificate validation and should not be used in production due to security risk.



Destinations Section

32. **IPAM Discovery:** Enable this if you want Aruba EdgeConnect networks and IPs to be written into Universal IPAM.
33. **Federated Realm: (Existing/New)** This option becomes available once the IPAM Discovery toggle is enabled. Select the destination Federated Realm (e.g., Default) where you want the discovered Aruba EdgeConnect networks to be created and managed. In most cases, a default realm is available for every tenant; however, you can also create a new realm directly from this screen and point Aruba EdgeConnect discovered networks to that realm instead.
34. **Tags: (Optional)** Add one or more tags to the Federated Realm to help classify, search, and report on IPAM destinations (e.g., environment, region, or business unit).

Note: Federated Realm is a unified framework within Infoblox Universal DDI designed to streamline the planning and enforcement of IP address usage across multiple IPAM platforms, including on-premises and cloud environments, like AWS, Azure, and Google, and third-party networks. It provides a single hierarchical view of an enterprise's network, enabling administrators to manage IP address blocks, apply policies, and maintain consistency across diverse infrastructure sources. This model simplifies operations by abstracting backend complexities and offering a user-centric interface for managing IPAM. For additional details on IPAM Federation, refer to [Configure IPAM Federation](#).

Destinations

IPAM Discovery Enabled

*Federated Realm

Existing New

Federated Realm

*Name

Description

[Add Tags](#)

[Save](#)

Tags Section

Use the **Tags** section to add, modify, or remove tags associated with the **Aruba EdgeConnect** discovery job. Tags can be used later for:

1. Grouping and searching discovery jobs.
2. Filtering or organizing jobs by environment (e.g., prod, staging, region-us-east).

Save the Discovery Job

After completing all the required sections:

1. Review the configuration for the Versa discovery job.
35. Click **Save** to complete the discovery job configuration.

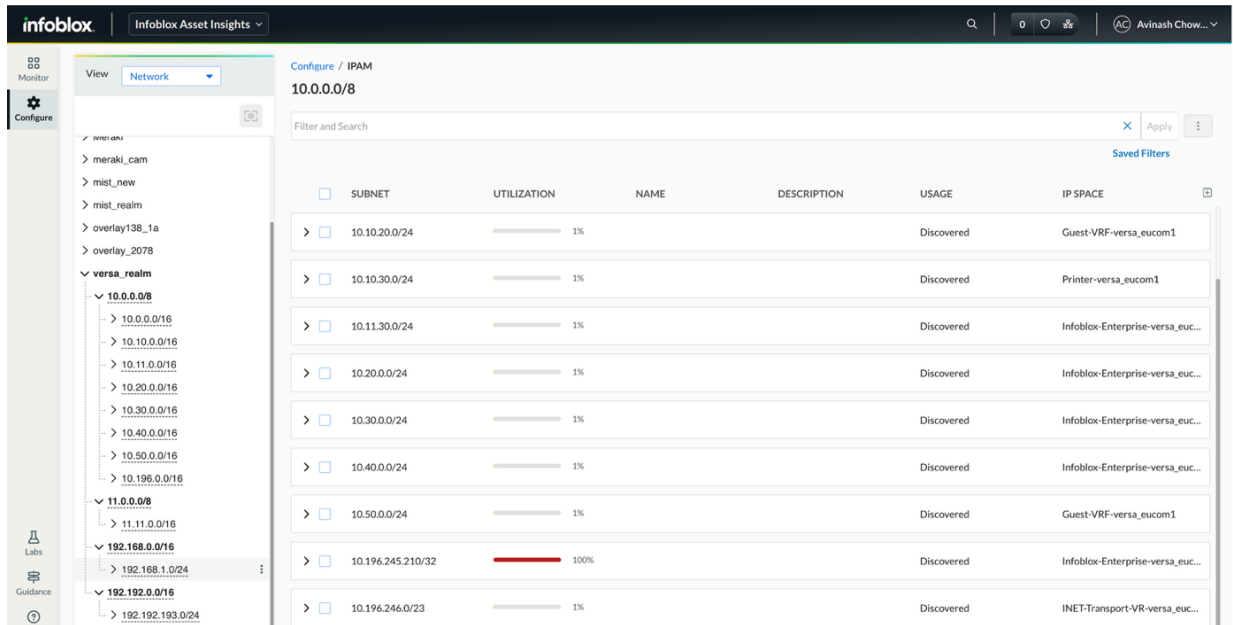
VIEW THE DISCOVERED DATA IN THE INFOBLOX PORTAL

Once the discovery jobs are created and sync is successful, follow these steps to view the discovered data for **Cisco Catalyst SD-WAN, Juniper Mist, Versa Networks, and Aruba EdgeConnect** in the Infoblox Portal.

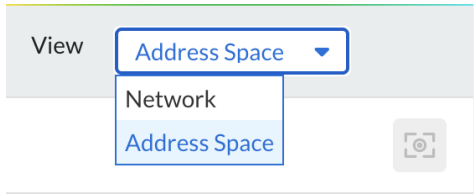
IPAM Data

Access New IPAM

1. Log in to the Infoblox Portal with an administrator account.
2. Go to the **Configure -> Networking -> IPAM (New)**. By default, New IPAM opens in the **Network Perspective**, which displays your IP space organized as networks and subnets rather than individual addresses. In this view, you can:
 36. See hierarchical blocks, networks, and subnets across on-prem, cloud, and third-party sources.



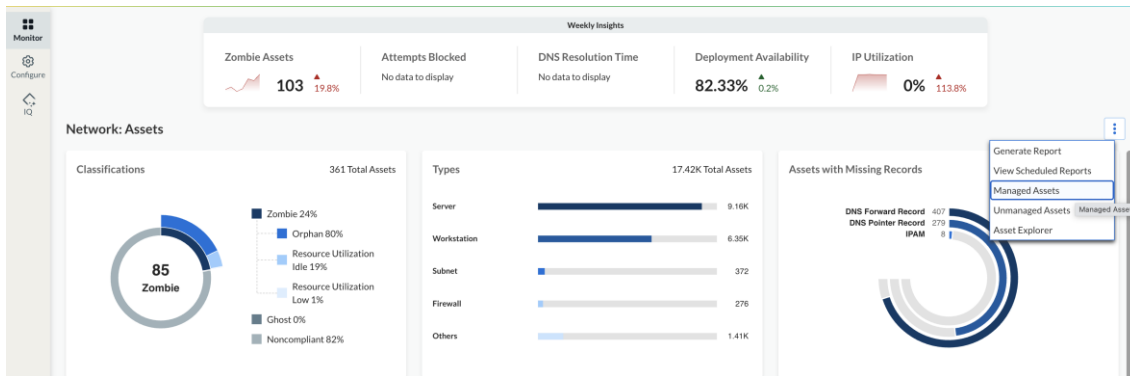
37. Use the **Filter** panel to narrow the view to networks discovered from these integrations—for example, by filtering on **Discovery job, Source, Subnet/Subnet Name, IP Address**, or relevant **Tags** to focus on networks coming from Cisco Catalyst SD-WAN, Juniper Mist, Versa Networks, or Aruba EdgeConnect and view information about the discovered devices.
38. Inspect utilization, hierarchy, and metadata for each network, helping you understand how SD-WAN, Mist, and Versa address space fits into your overall IP plan.
39. **Address Space** perspective is a view mode in Infoblox's new IPAM that lets users visualize and manage IP resources organized by address space, as an alternative to the Network-based view. In this view, you can:



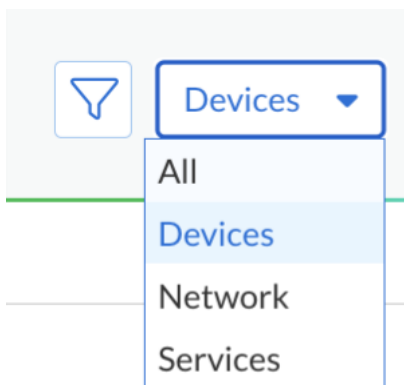
- a. See each IP address, its status (used/unused), and associated metadata (hostname, lease, device, etc.).
- b. Apply filters to narrow down results by specific criteria such as IP range, status, or tags.
- c. Drill into a given IP to understand which SD-WAN edge, Mist AP/client, or Versa device is using it, supporting troubleshooting, forensics, and IP reconciliation across third-party platforms.

Asset Inventory Data

1. Click on **Monitor**, which takes you to the **Network -> DDI** sub-workspace by default. Click **Assets** to switch to **Network -> Assets** sub-workspace. From the ellipses, click **Managed Assets**.



2. This opens **Devices** by default. Select **All**.



3. Click the **Filter** button and select the **provider** as Cisco Catalyst SD-WAN, Juniper Mist, Versa Networks, Aruba EdgeConnect or any combination of these. Click **Apply**. The Asset Inventory will then display assets for the provider(s) you selected, allowing you to:
 - a. See which devices and clients are present at each site and how they are connected.

- b. Pivot from an asset to its IP addresses, subnets, and related infrastructure for faster troubleshooting.
- c. Export filtered views for reporting, audits, or CMDB reconciliation.
- d. Compare provider specific views (e.g., SD-WAN edges vs. Mist access points vs. Versa devices vs Aruba EdgeConnect devices) to identify gaps, overlaps, or stale entries across your environment.

The screenshot displays the 'Asset Inventory' page in the Infoblox Universal Asset Insights interface. The main table lists various assets with columns for Name, Vendor, Location, Type, IP Address, Providers, Model, MAC Address, and Operating System. The right-hand side features a summary dashboard with a donut chart showing 886 total assets, categorized by type: Server (3%), End User Device (17%), Laptop (20%), and Unclassified (20%). Other categories include Others (36%) and Assets with Missing Records (No data to display). A 'Locations' section shows a breakdown: Unassigned (47%), Others (36%), HQ Bu... (6%), and 3% H... (3%). The interface also includes navigation options like 'Save', 'Apply', and 'All' at the top right, and a 'Providers' dropdown menu at the bottom right.

Name	Vendor	Location	Type	IP Address	Providers	Model	MAC Address	Operating System
LAPTOP-P1NO	HPE	HQ-Building A - 2nd Fl...	Laptop	10.10.1.88		EliteBook	10B6:7684:5F:86	Windows 11
PIXEL-ZAMK	Google	HQ-Building A - 2nd Fl...	End User Device	10.10.1.15		Pixel	F4:F5:D8:FC:44:EF	Android 14
MACBOOK-KG68	Apple	HQ-Building A - 1st Flo...	Laptop	10.10.1.110		MacBook	A4:83:E7:53:4A:5B	macOS Ventura
THINKPAD-RM7P	Lenovo	HQ-Building A - 1st Flo...	Laptop	10.10.1.26		ThinkPad	28:D2:44:78:26:AE	Windows 10
GALAXY-KH2T	Samsung	HQ-Building B - 1st Flo...	End User Device	10.10.2.56		Galaxy	84:25:D8:5E:01:51	Android 14
Versa-onprem-Lingesh	Versa Networks	US	Gateway	10.0.9.244		Standard PC (i440FX + ...	-	VOS
ec-branch-syd	HPE	Site-SYD	Router	10.1.12.1 +3 more		EC-10106	00:50:56:00:0B:00 +3...	EdgeConnect OS
PM-TEST-04	Versa Networks	mexico	Gateway	10.0.10.212		Standard PC (i440FX + ...	-	VOS
ec-hub-apac	HPE	Site-SING-HUB	Router	10.1.16.1 +3 more		Ec-l	00:50:56:00:0F:00 +3...	EdgeConnect OS
demo-exec	Versa Networks	Nuukie, Karnataka, India	Gateway	10.0.9.232		Standard PC (i440FX + ...	-	VOS
ec-branch-tok	HPE	Site-TOK	Router	10.1.11.1 +3 more		EC-10104	00:50:56:00:0A:00 +3...	EdgeConnect OS
TEST-2WAN	Versa Networks	Pune, Maharashtra, India	Switch	10.0.0.27 +11 more		CAF-0262	08:35:71:A9:87:08 +2...	VOS
ec-hub-emea	HPE	Site-FRA-HUB	Router	10.1.9.1 +3 more		EC-10150	00:50:56:00:08:00 +3...	EdgeConnect OS
ec-branch-mia	HPE	Site-MIA	Router	10.1.18.1 +3 more		Ec-us	00:50:56:00:11:00 +3...	EdgeConnect OS
ec-branch-dfw	HPE	Site-DFW	Router	10.1.17.1 +3 more		EC-10106	00:50:56:00:10:00 +3...	EdgeConnect OS
HALO-DEMO	Versa Networks	BENGALURU, Karnata...	Switch	10.0.12.164		Standard PC (i440FX + ...	-	VOS
ec-branch-par	HPE	Site-PAR	Router	10.1.14.1 +3 more		Ec-xs	00:50:56:00:0D:00 +3...	EdgeConnect OS
ec-branch-lax	HPE	Site-LAX	Router	10.1.4.1 +3 more		Ec-s	00:50:56:00:03:00 +3...	EdgeConnect OS
working-session-6	Versa Networks	BENGALURU, Karnata...	Switch	10.0.12.106		Standard PC (i440FX + ...	-	VOS



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