appviewx

# DDI+ Guides

**Version: 2025.0.0.0**

# Copyright AppViewX, Inc.



## Trademarks



## Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

# Contents

# Preface

## Revision History

| Revision | Description | Date |
|---|---|---|
| 1.0 | Initial draft of document for release 2025.0.0.0 | November 2025 |

## About this Guide

This section includes the following guides.

- DDI+ User Guide
- DDI+ Admin Guide

## Audience

This guide is designed for DNS administrators and Network Operations (NetOps) teams.

## Third-Party Software Acknowledgments

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

## Text Conventions

The following text conventions are used in this document:

| Convention | Description |
|---|---|
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `codeblock` | Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter. |

# Chapter 1: DDI+ User Guide

This guide describes the process of domain lifecycle management starting from integrating the domain registrars, procuring and syncing the domain, to renewing, managing, and decommissioning domains.



## Introduction

DDI+ is a centralized platform designed to simplify and secure the enterprise DNS ecosystem. Experience the convenience of a unified solution seamlessly integrating Domain registrars, DNS, IP Address Management, Load Balancers, Firewalls, and Configuration Management Database (CMDB) assets to streamline the DNS and Domain lifecycle management.

### DDI+ Features

**Centralised Control and Governance**

• Centralized Management of Domain Registrars, DNS, and IPAM.

• Single Source of Truth (SSOT) for Domains, DNS, IPs, Load balancer, and Firewalls

**Visibility and Control**

• App-centric visibility across DNS, IP, Load Balancers, and Firewalls

• Insights into Domain Expiry and DNSSEC keys (ZSK and KSK)

• IP and CMDB asset violation report

• IP Hygiene Compliance and Remediation

**Self-service and Automation**

- Automate Domain Lifecycle Management (Domain Procurement, Renewal, Modification, and Create Hosted Zones)
- Automate IPAM and DNS Provisioning

**Reports**

- Orphan/Rouge IP Report
- DNS Traffic utilization
- DNSSEC Keys expiry and rollover
- ADC vs IPAM violation report

# Getting Started

## Know your Deployments for DDI+

We support multiple deployment options to cater to various customer needs and infrastructure preferences. Our solutions can be deployed in On-Premises environments, Managed Kubernetes platforms such as EKS, AKS, GKE and OpenShift and as a Software as a Service (SaaS).

| **SaaS Deployment (Highly Secure and Hassle-Free)** |
| --- |
| Our Software as a Service (SaaS) offering is designed for organizations that prioritize security, simplicity, and efficiency. In this deployment mode, we manage all aspects of application hosting, maintenance, and scaling, providing a worry-free experience for our customers. Our SaaS platform is built with cutting-edge security measures, including robust encryption, multi-factor authentication, and continuous monitoring to ensure your data and operations are protected at all times.<br><br>Choosing SaaS not only reduces the burden on your IT teams but also ensures that you benefit from the latest updates, features, and security enhancements without any additional effort. This option is ideal for organizations of all sizes, particularly those looking to quickly access our services with the assurance of enterprise-grade security and compliance.<br>For additional information about saas deployment, click here. |
| **On-Premises Deployment** |

On-Premises deployment enables organizations to install and operate our applications on their own infrastructure. This approach offers the highest level of control and customization, making it particularly suitable for organizations with strict security, compliance, or performance needs. It is best suited for enterprises with dedicated IT resources and the expertise to manage complex infrastructure. For additional information about on-premises deployment, click here.

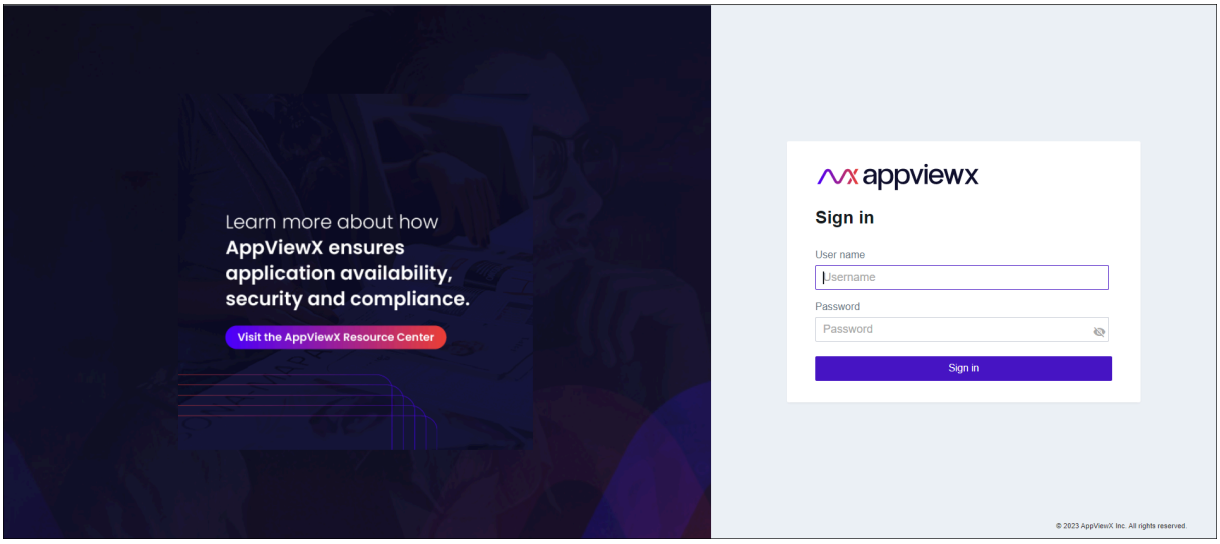
**Managed Kubernetes Deployment (AKS, EKS, and GKE)**

We offer support for deployment on Managed Kubernetes services such as Amazon EKS, Microsoft AKS, and Google GKE. Managed Kubernetes platforms simplify the management of Kubernetes clusters by handling tasks like cluster provisioning, maintenance, and scaling. This deployment option is suitable for organizations looking for a balance between control and operational simplicity, and for those who prefer leveraging cloud providers' infrastructure and expertise. For additional information about managed kubernetes deployment, click here.



## Accessing the DDI+ Module

1. Log into AppViewX with a valid credential (URL provided by AppViewX).
   The AppViewX Landing page appears.



2. Go to (**Menu**) > **DDI+** .

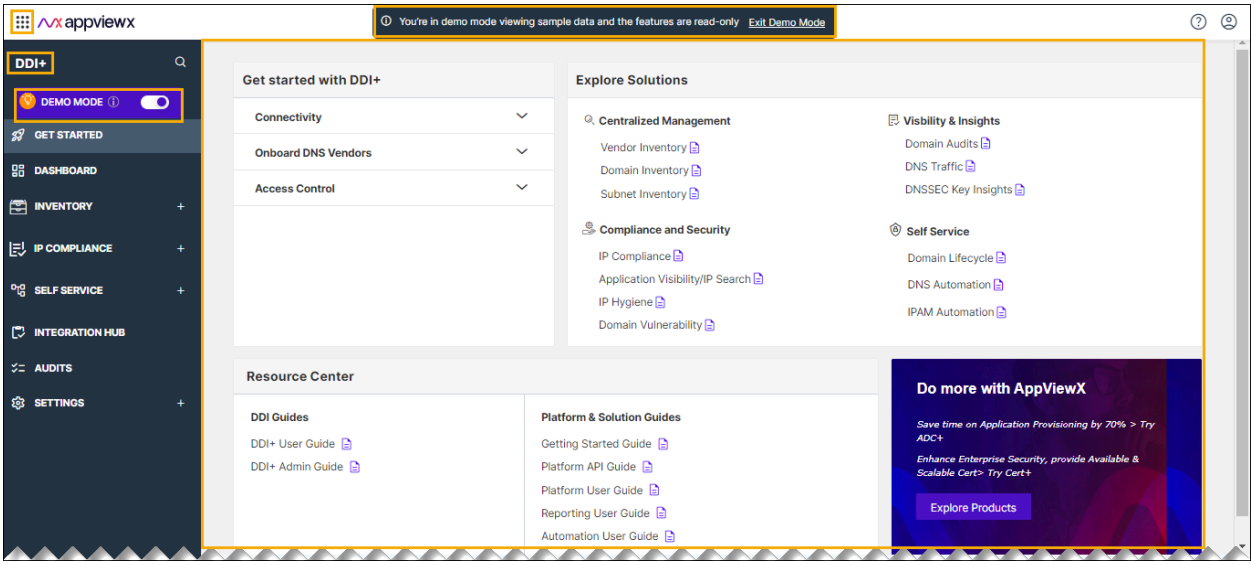
   The **DDI+** module is displayed with the **Get Started** section open by default.

## Demo Mode

Demo Mode is a state in which the DDI+ system operates to showcase its capabilities and features in a controlled environment. In Demo Mode, you can explore all DDI+ features with sample data, but you will not be able to perform any actions.

The Demo Mode feature option can be found within the left navigation panel. You have the flexibility to enable or disable this feature according to your requirements. Availability of other DDI+ features in Demo Mode might vary depending on the permissions set by the Access Control Framework (ACF).

To access the Demo Mode, Navigate to **Menu** > **DDI+** and, then click the **DEMO MODE** toggle button. While in Demo Mode, you will notice that the Demo Mode option in the left navigation panel is highlighted. Additionally, there will be a banner displaying content indicating that you are currently in Demo Mode.




### Enabling Demo Mode

To enable the Demo Mode:

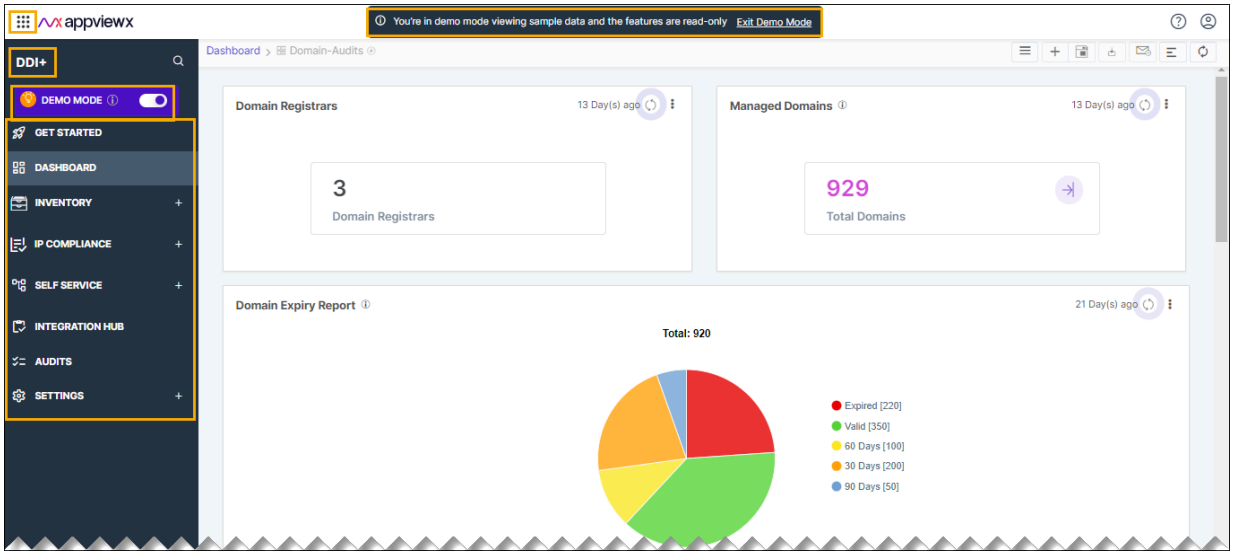
1. Go to **Menu** > **DDI+**.
2. Click the Demo Mode toggle button.

   The Demo Mode option in the left navigation panel is highlighted and a notification message displayed on the banner, indicating that the Demo Mode has been enabled.

## Understanding Features in Demo Mode

Though you can not perform any actions within DDI+ while in Demo mode, you can still experience how the output appears for each action performed on the device/object.

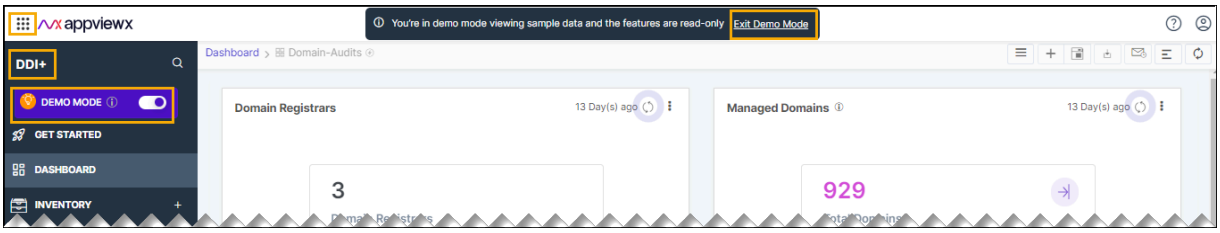
- GET STARTED
- DASBOARD
- INVENTORY
- IP COMPLIANCE
- SELF SERVICE
- INTEGRATION HUB
- AUDITS
- SETTINGS.




## Exiting Demo Mode

To exit from the Demo Mode:

1. Go to **Menu** > **DDI+**.
2. Click the Demo Mode toggle button.




The highlight sign on the Demo Mode option in the left navigation panel disappears and the notification message displayed on the banner also disappears.

## Application Topology

The application topology enables you to get a holistic insight into your application. It enables you to visualize the entire setup, including DNS entries, server pools, and the firewall. The application topology page initially displays a topology map illustrating all services within a specific icon (application) and their interconnections.

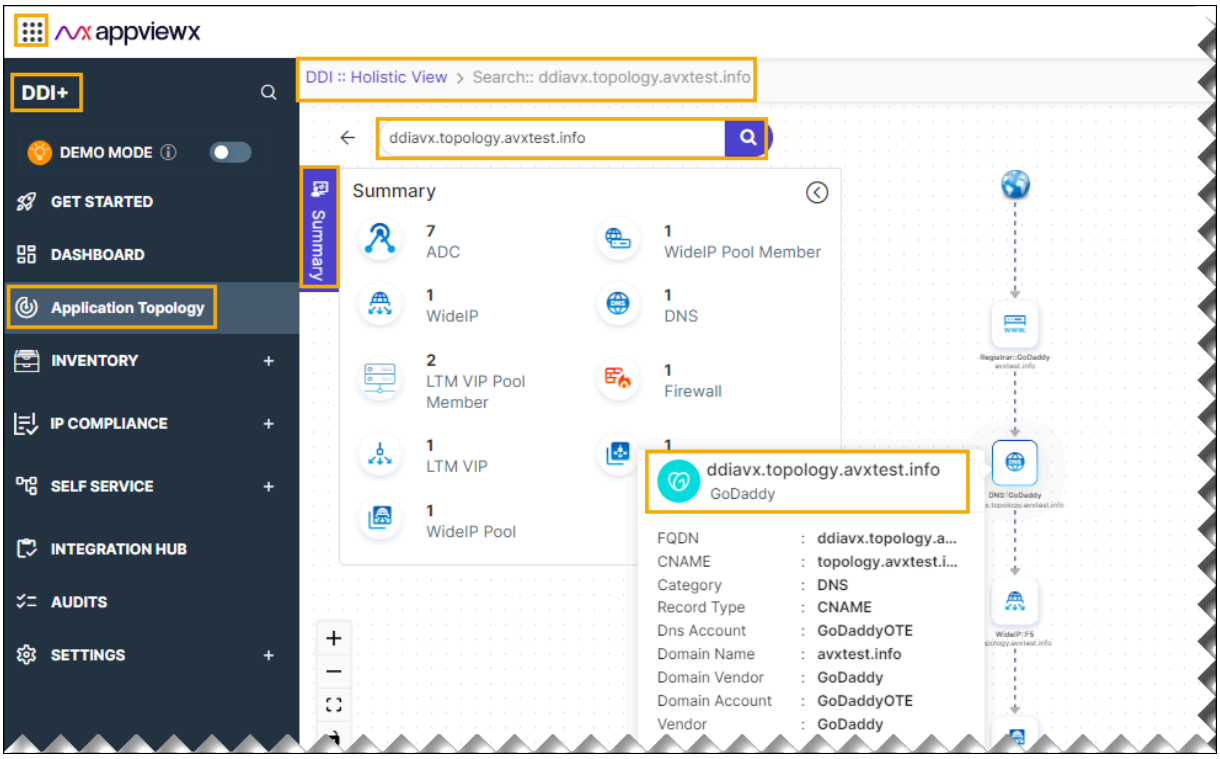
To access the application topology, do the following steps.

1. Go to **DDI+** > **APPLICATION TOPOLOGY**.

   The **Holistic View** page is displayed.

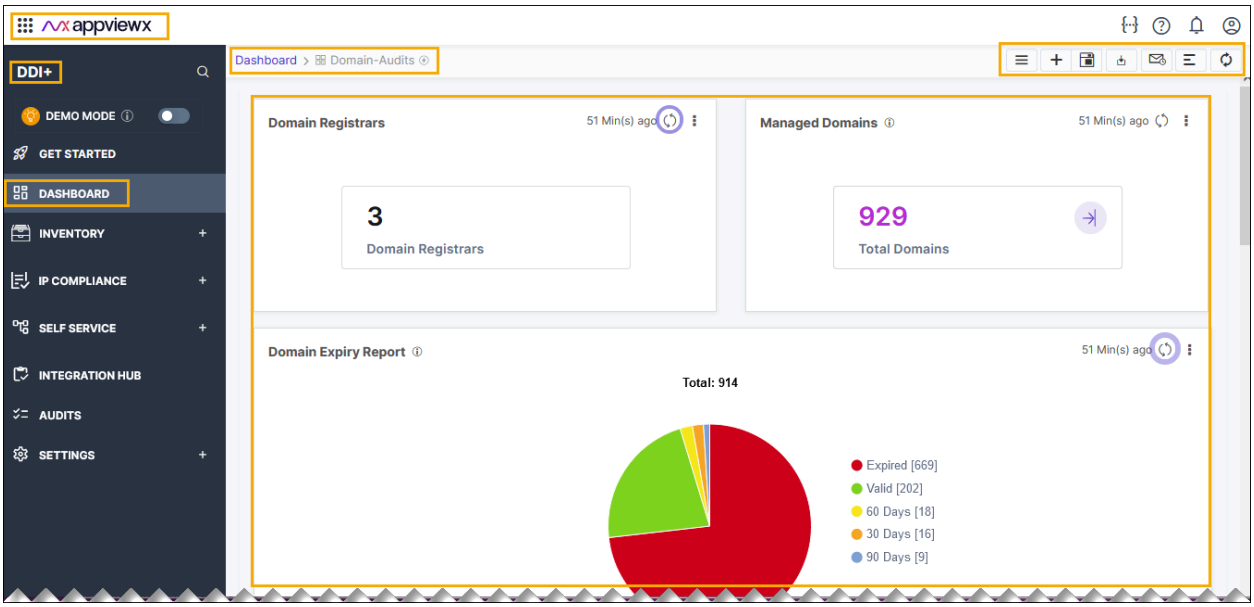
2. Enter the domain name in the search field, and then click **Search**.

The application topology **Summary** page is displayed.




## Getting Started with Dashboard

The DDI+ module dashboard provides a comprehensive summary of metrics including Domain Audits, IP Compliance, DNS Zone Traffic Reports, F5 DNS Security Reports, Microsoft DNS Audits, and Domain Vulnerability Insights. You can access the features under **DASHBOARD** from the left menu.




- **Dashboards** - Dashboard display reports and widgets that provides consolidated statistics of all data from the respective inventories and recording the key value indicators. The following table describes the options available on this dashboard:

| Options | Description |
|---|---|
| **Dashboard name** | Displays the name of the current dashboard. |
| **Options** | **Description** |
|  | Allows you to navigate to the Dashboard inventory. |
| **Options** | **Description** |
|  | Allows you to create a dashboard/widget. |
| **Options** | **Description** |
|  | Allows you to save the dashboard. |
| **Options** | **Description** |
|  | Allows to download the dashboard details in the <.pdf> format. |
| **Options** | **Description** |
|  | Allows you to align the widgets on the dashboard. |
| **Options** | **Description** |
|  | Refreshes the dashboard. |

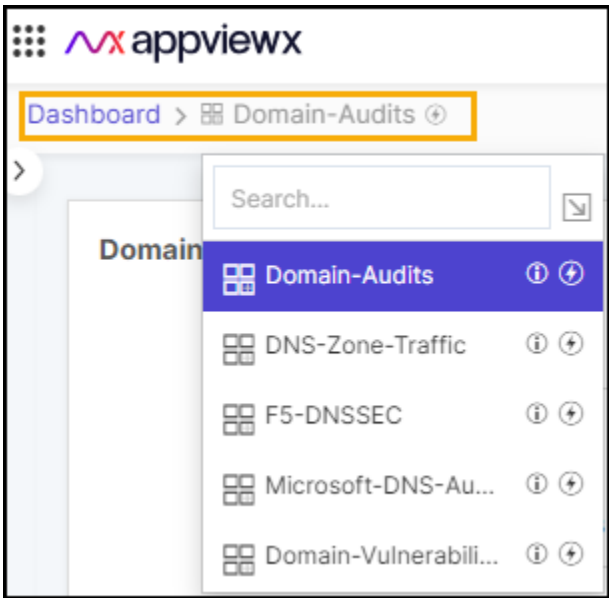
## Accessing the Dashboard

To access the dashboard:

1. Go to **Menu** > **DDI+** > **DASHBOARD**.

   The dashboard home page appears.

2. Move your cursor to the breadcrumbs field of the current dashboard.
3. Click the current dashboard name.
4. In the dropdown list that appears, click the name of the dashboard you want to view.

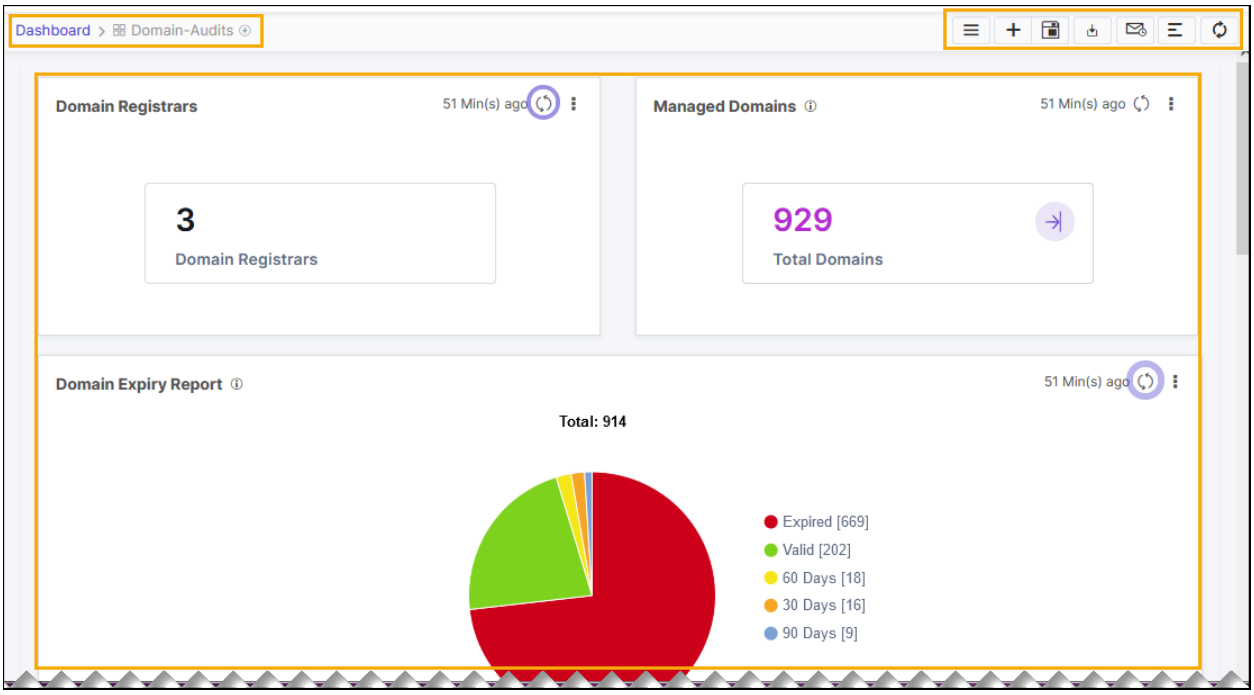



**Note:** You can also click the ☰ (**Dashboard inventory**) button in the Command Bar and click the name of the dashboard you want to switch to.

- Domain Audits
- DNS Zone Traffic Reports
- F5 DNS Security Reports
- Microsoft DNS Audits
- Domain Vulnerability Insights
- Downloading and Exporting the Dashboard Reports

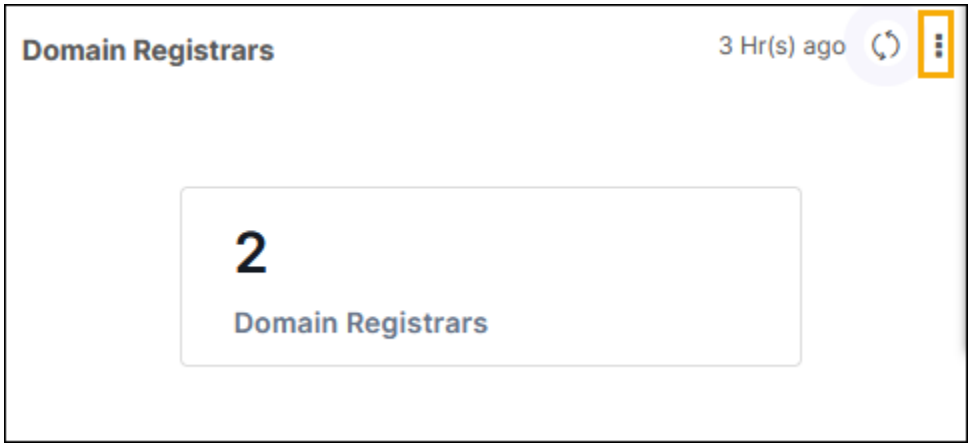
## Domain Audits

Domain audits dashboard provides a comprehensive overview of domain landscape in an enterprise. Track the total count of managed domains, get expiry reports, and analyze expiration trends. Additionally, explore the distribution of domains across various top-level domains (TLDs).

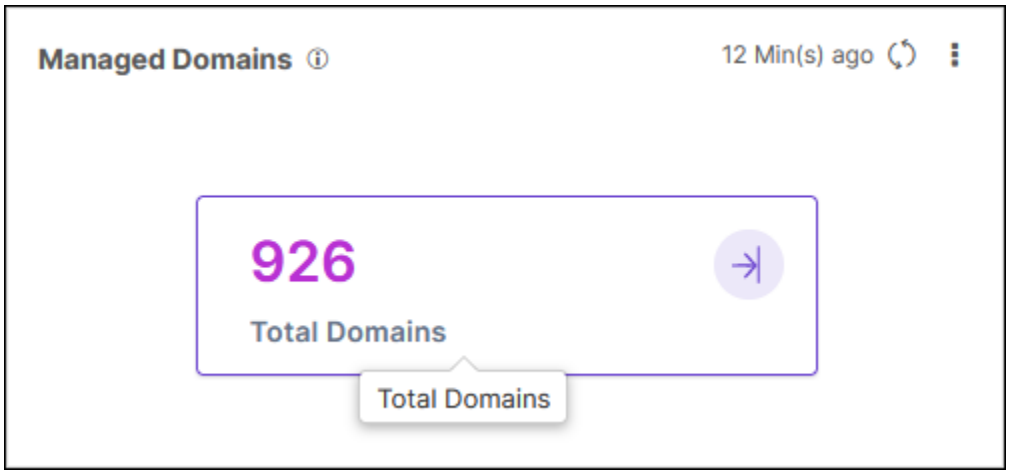



The following reports are available under the **Domain Audits** tab:

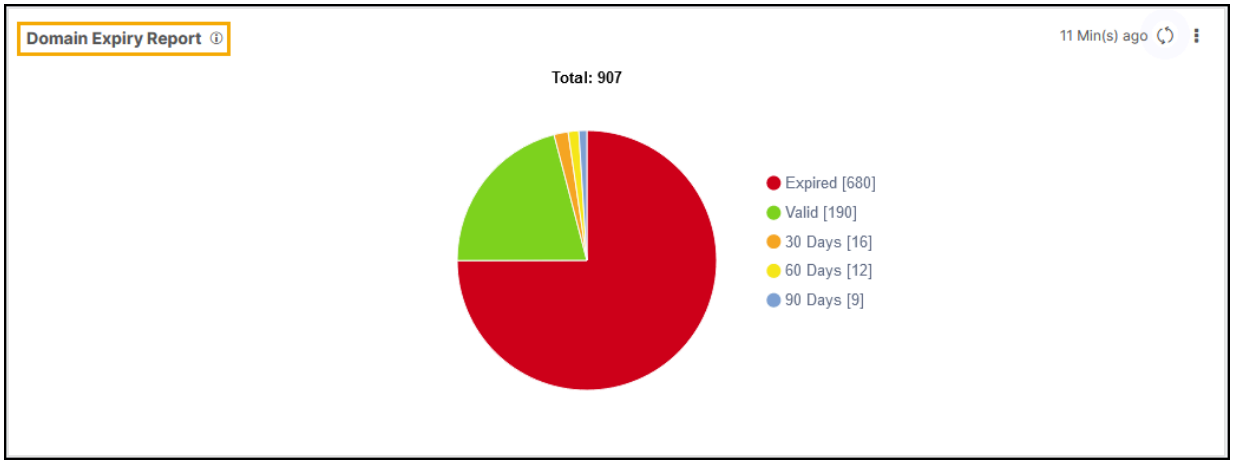
- **Domain Registrars**: This metric displays the total number of domain registrars configured in DDI+ integration hub.



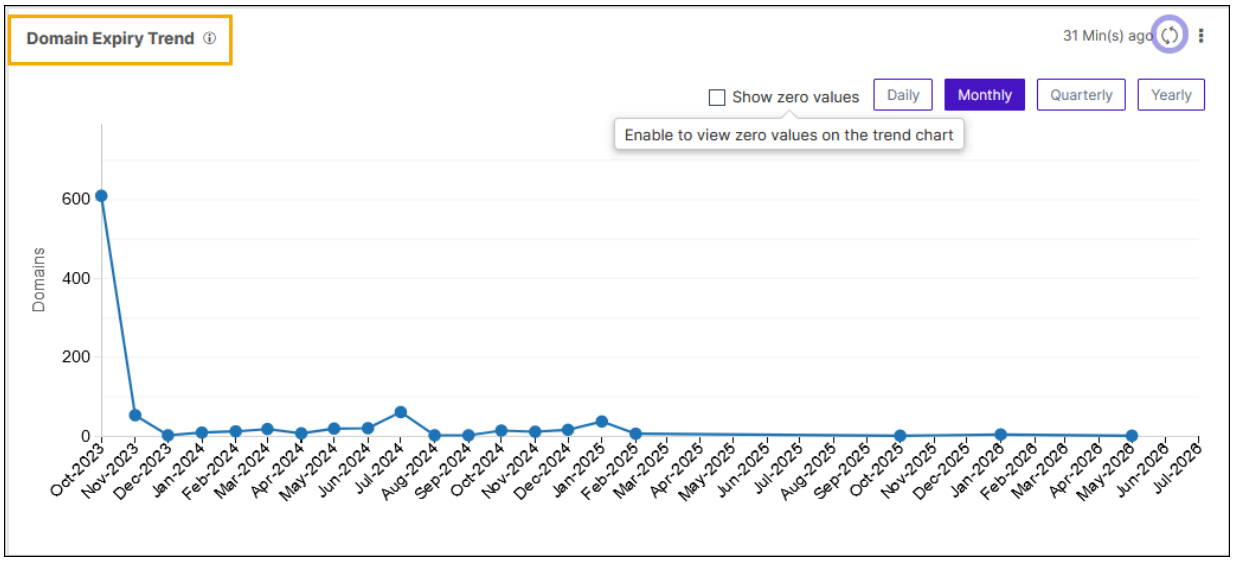

- **Managed Domains**: This metric displays the total number of managed domains in the inventory.



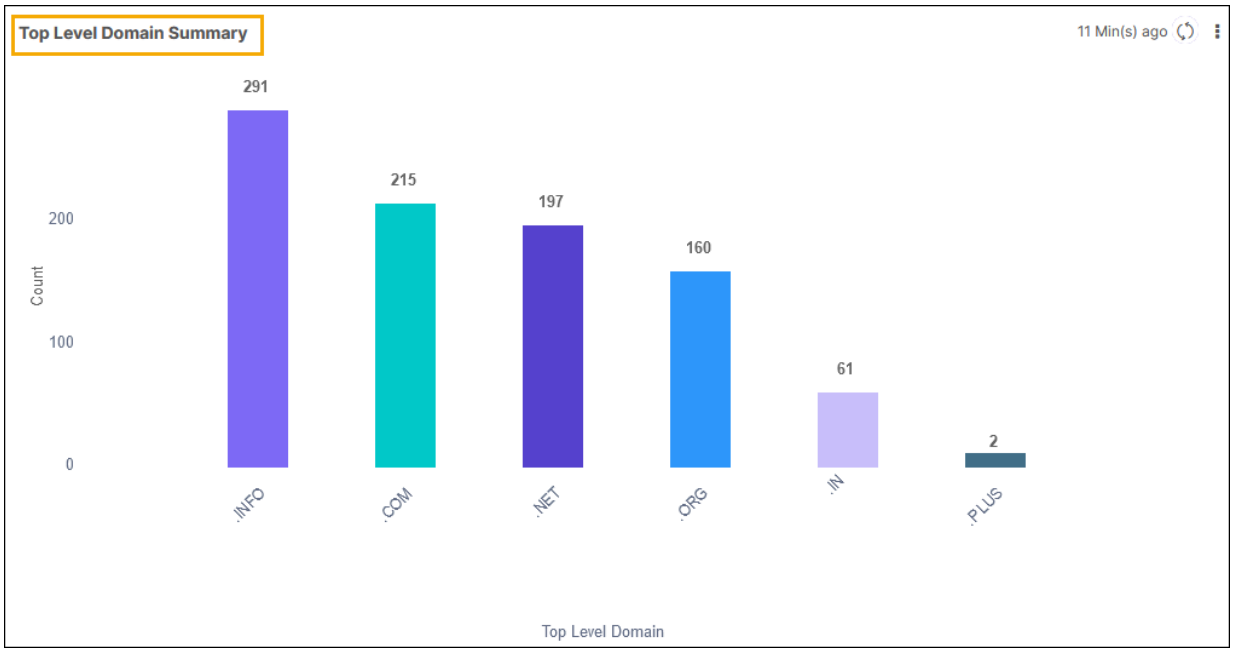

- **Domain Expiry Report**: This report displays the expiry status of the domains. The different colored sections of the pie represent the status of the domains with respect to expiry. For example: valid, expired, expiring in 30 days, 60 days, and 90 days.




- **Domain Expiry Trend**: This trend line chart illustrates the monthly, yearly, and quarterly trends of domain expiry.



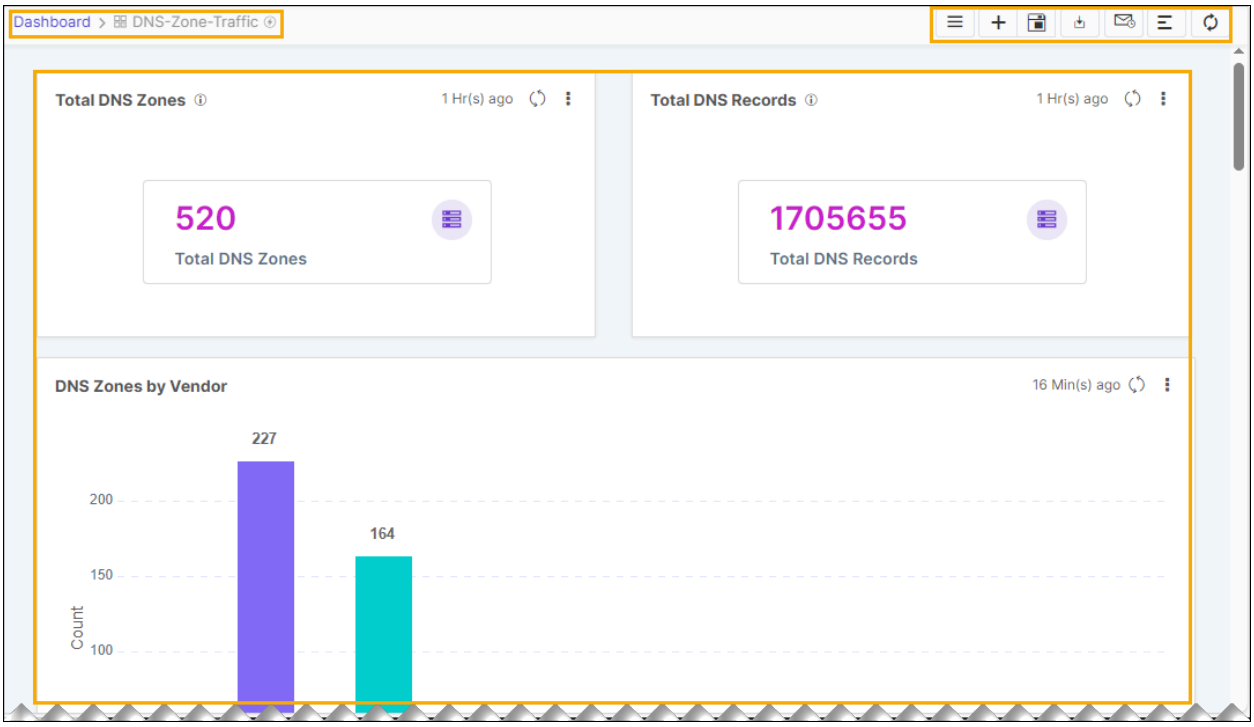

- **Top Level Domain Summary**: This report offers a view of the number of domains categorized by Top-Level Domain (TLD).




**Note:** You can click on the corresponding metric to view the detailed information.

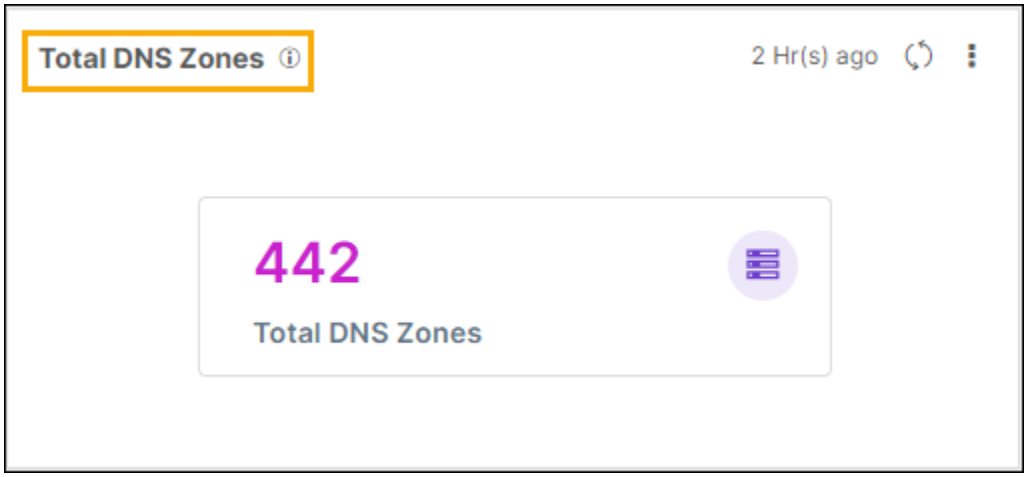
## DNS Zone Traffic Reports

In this dashboard users can get insights into the DNS landscape, traffic information, and across multiple DNS Vendors.

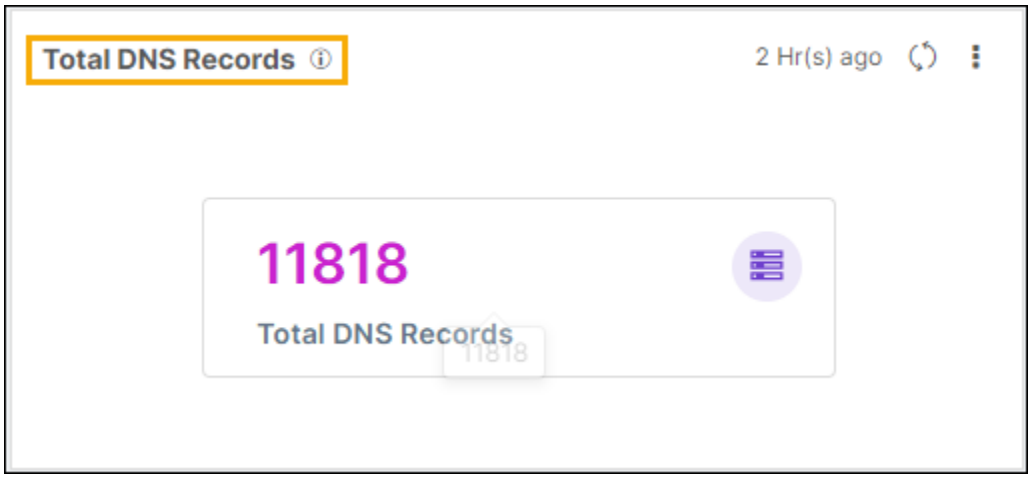



The following reports are available under the **DNS Zone Traffic** tab:

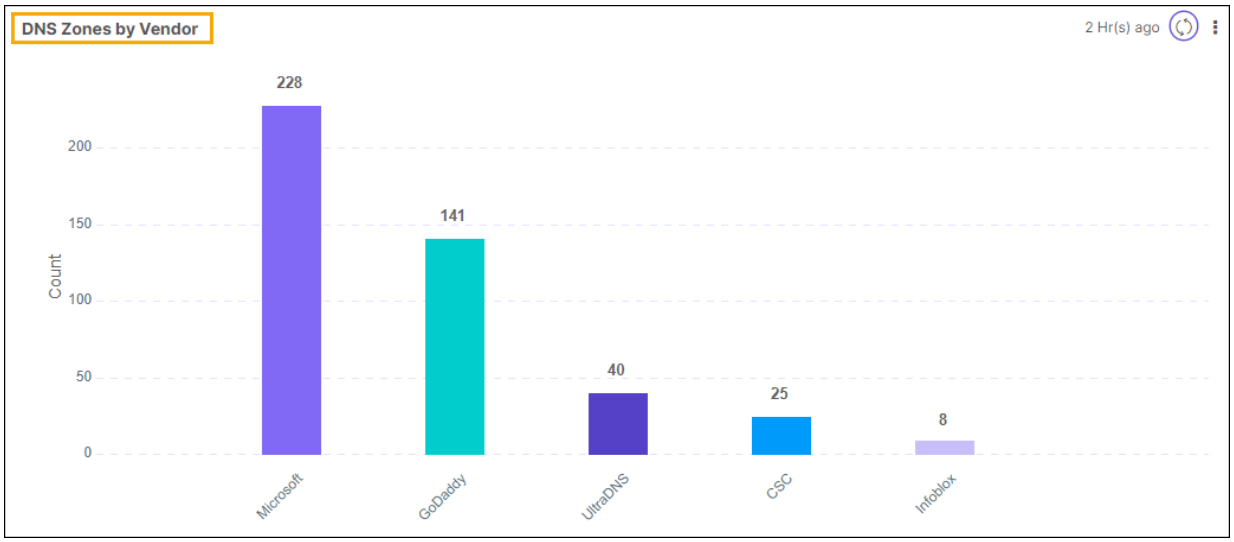
- **Total DNS Zones**: This metric displays the total number of DNS zones managed in the inventory across DNS vendors.



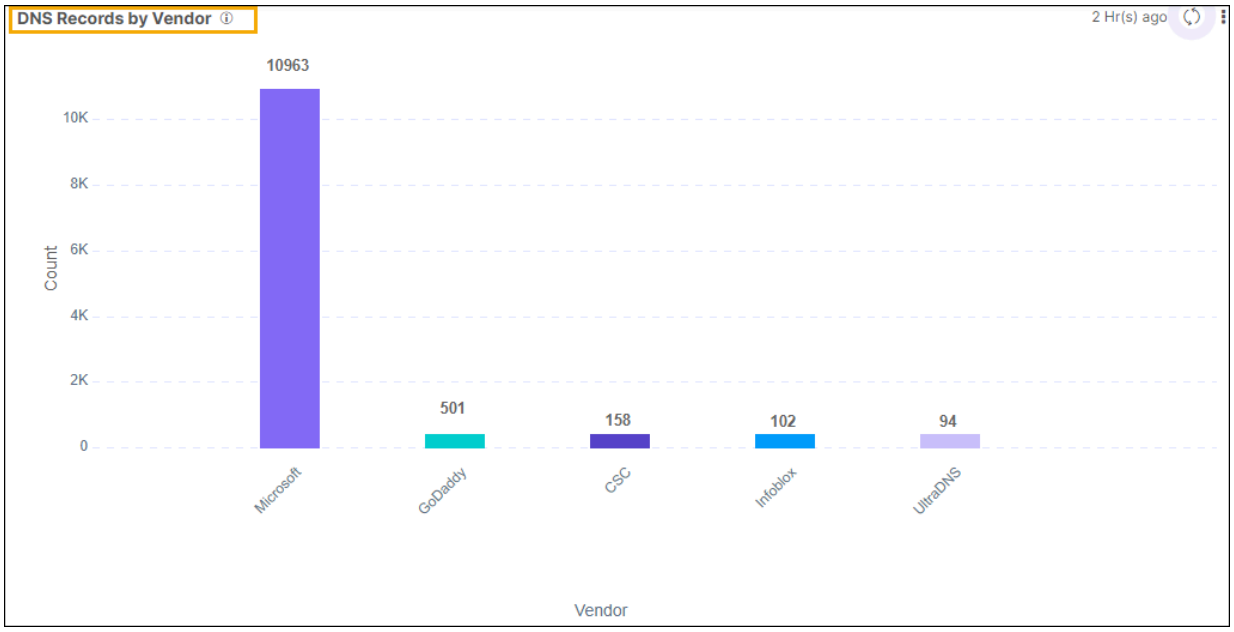

- **Total DNS Records**: This metric displays the total number of DNS records managed in the inventory across DNS vendors.



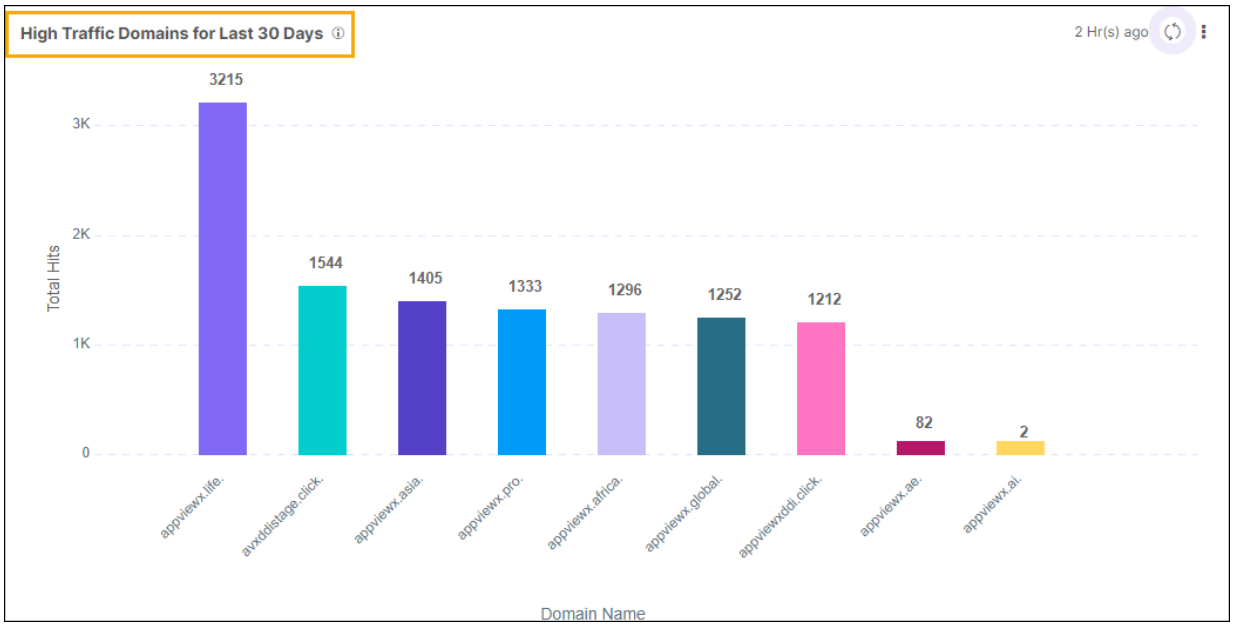

- **DNS Zones by Vendor:** This report displays the number of zones registered by vendor. The X-axis represents the names of the vendors and Y-axis represents the number zones per vendor.



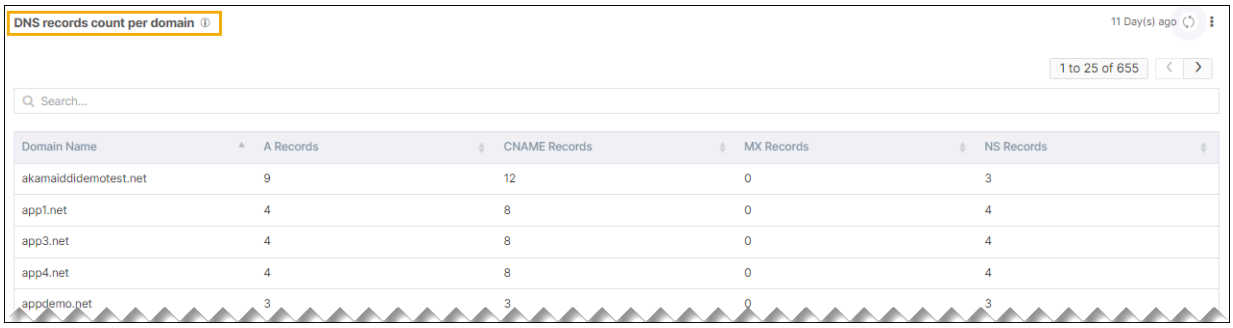

- **DNS Records by Vendor**: This report displays the total number of DNS Records managed across DNS vendors configured in the integration hub. The X-axis displays the names of the vendors and Y-axis represents the number of DNS records.



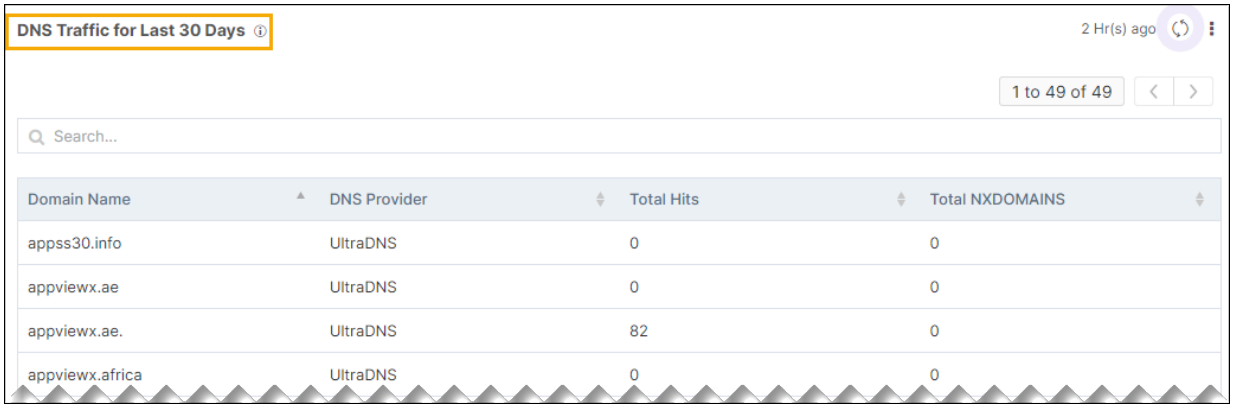

- **High Traffic Domains for Last 30 Days**: This graph displays information about the domains that received high traffic in the last 30 days. The X-axis represents the domain names and Y-axis represents the number of hits to the domain (in thousands).




- **DNS records count per domain:** This grid displays information about the number of DNS records for each domain. Only 25 records are displayed at a time. You can use the pagination arrows to view more records. Type the domain name in the search bar for DNS records information for that domain.



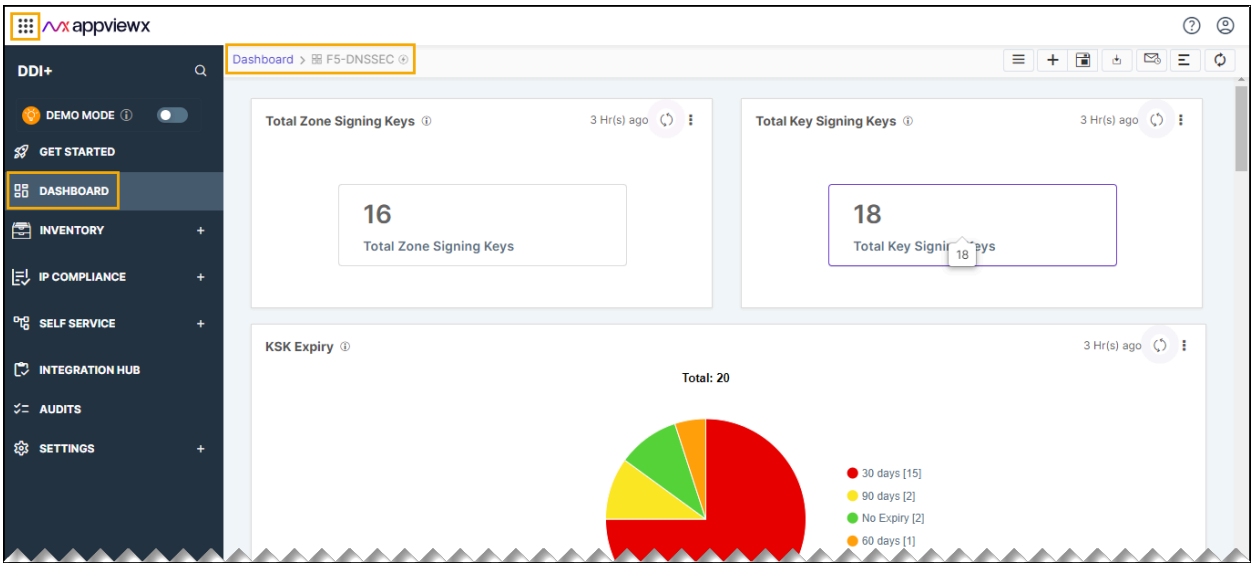

- **DNS Traffic for Last 30 Days**: This grid displays information on the traffic hits on all domains in the last 30 days. Only 25 records are displayed at a time. You can use the pagination arrows to view more records. Type the domain in the search bar for expiry information about a specific domain.




**Note:** You can click on the corresponding metric to view the detailed information.

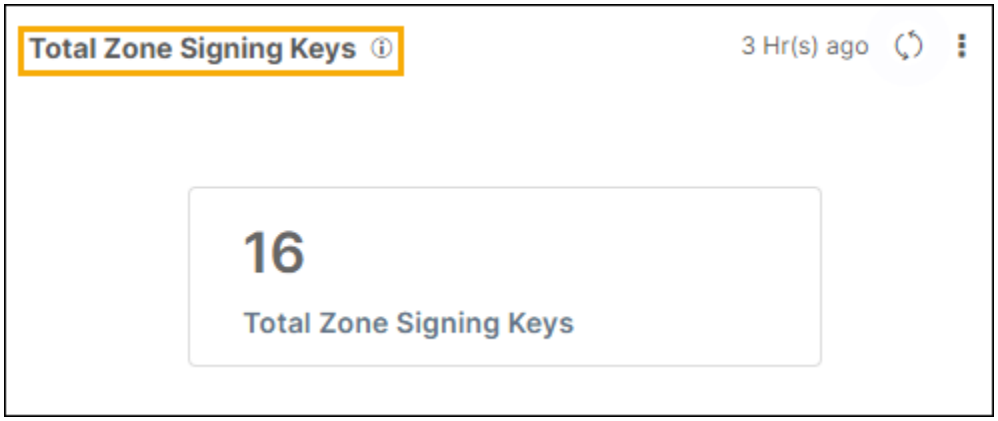
## F5 DNS Security Reports

The DNSSEC Dashboard for F5 offers visibility and insights into the management of DNSSEC Keys within F5 DNS. It provides information on the expiration status of KSK keys and trends regarding their expiry. Additionally, it presents a single view of the mapping between Zones and keys.

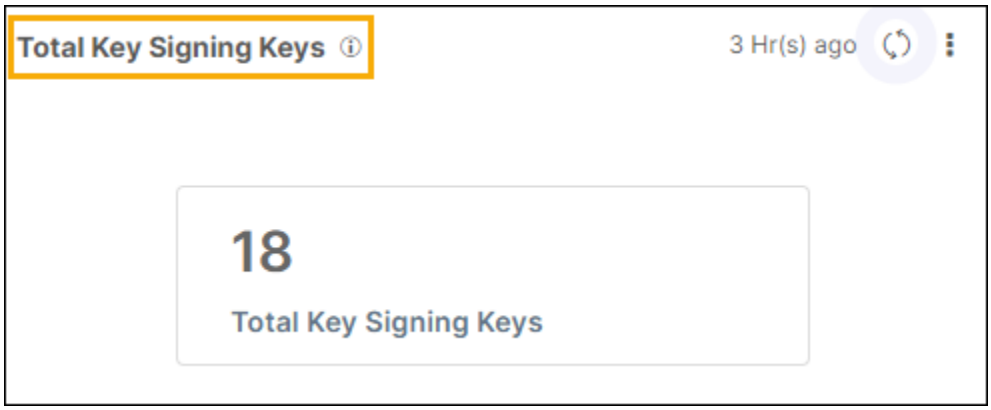



The following reports are available under the **F5_DNSSEC** tab:

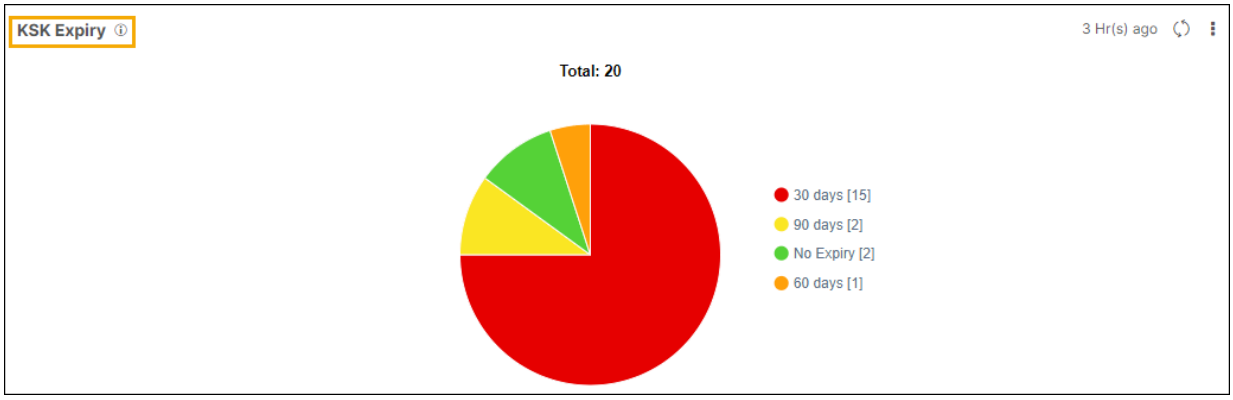
- **Total Zone Signing Keys**: This metric displays the total number of Zone Signing Keys present across the F5 DNS managed in AppViewX.



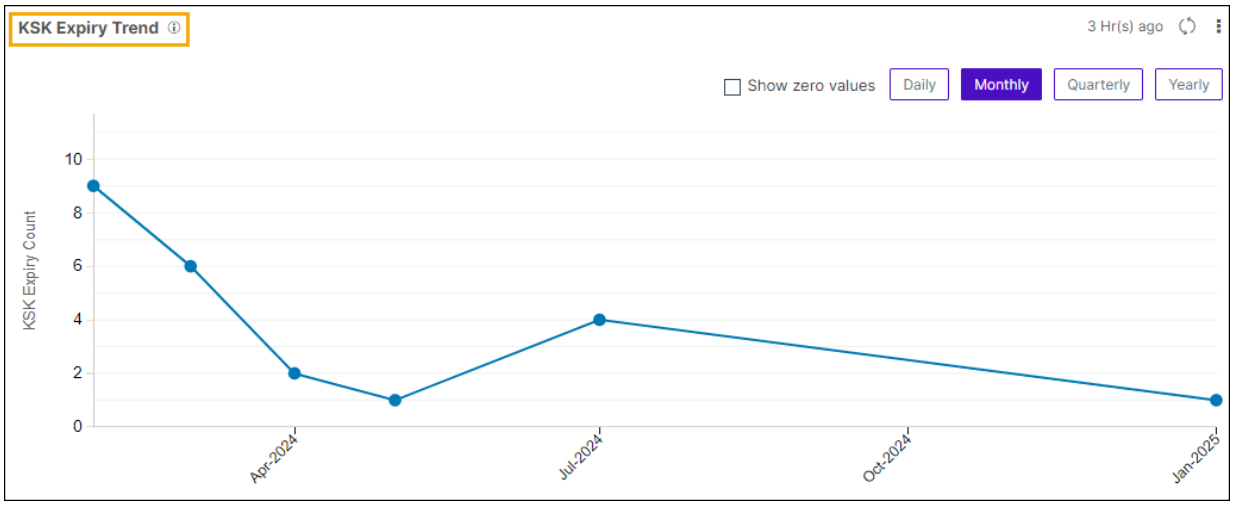

- **Total Key Signing Keys**: This metric displays the total number of Key signing key present across the F5 DNS managed in AppViewX.



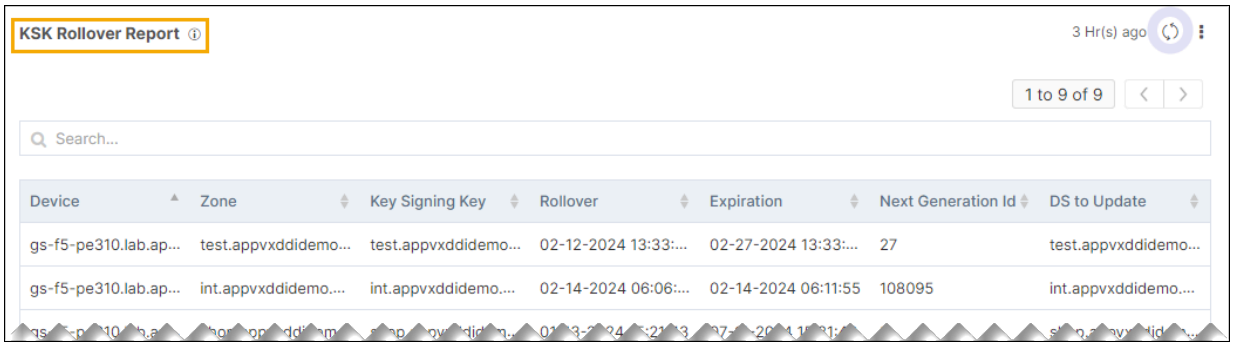

- **KSK Expiry**: This report displays the expiry status of the key signing keys. The different colored sections of the pie represent the expiry status of the KSKs. For example: valid, expired ,expiring in 30 days, 60 days, and 90 days.



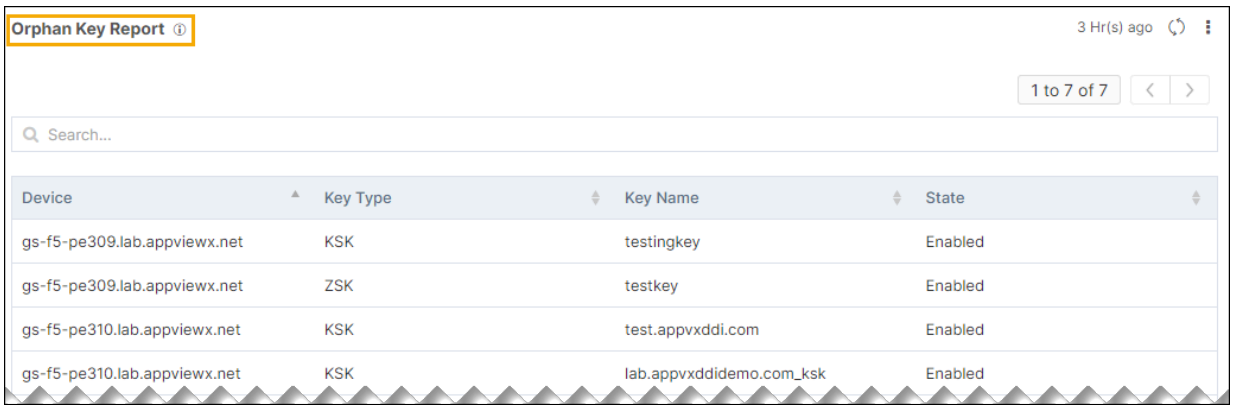

- **KSK Expiry Trend**: This report displays the expiry trend of the key signing keys.



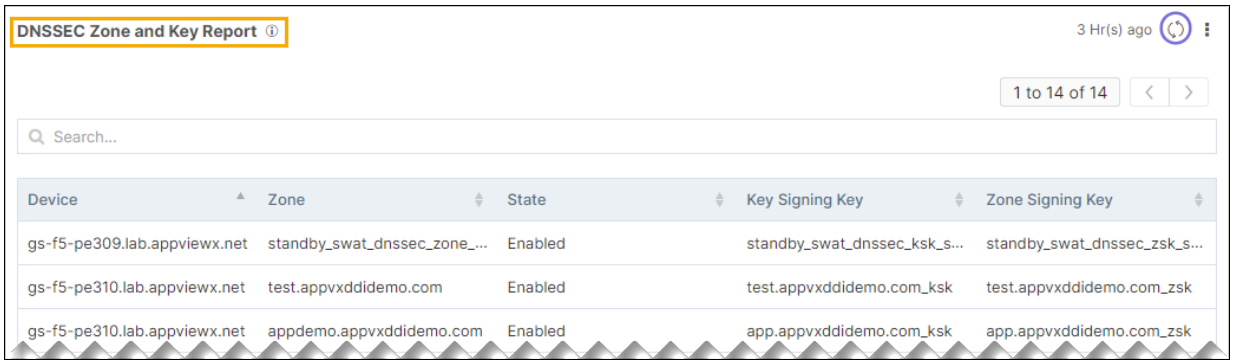

- **KSK Rollover Report**: The following grid displays the rollover and expiry dates for the KSKs along with the DS record that needs to be updated.




- **Orphan Key Report**: This report displays the key signing keys and zone signing keys that are not associated with any zone. The grid displays the name of the key(s) along with their status.



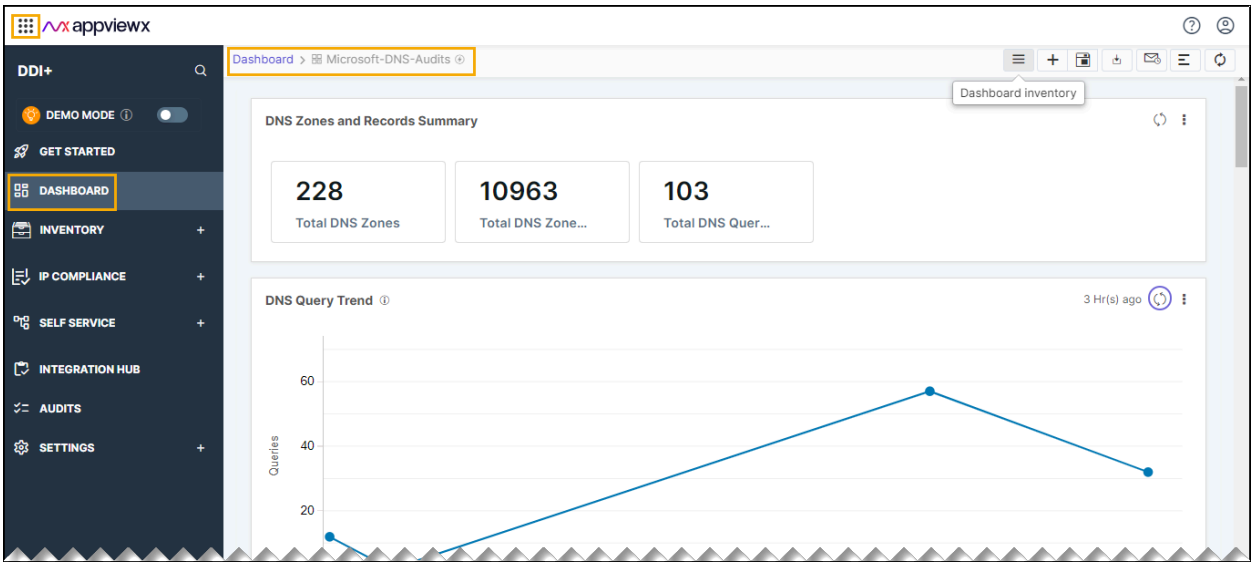

- **DNSSEC Zone and Key Report**: The DNSSEC zone and key grid displays all the zones with information on their status (enabled/disabled) and the associated Zone Signing Key and Key Signing Key.




**Note:** You can click on the corresponding metric to view the detailed information.

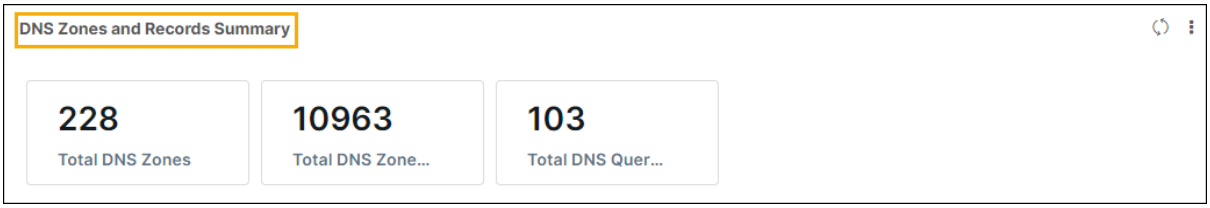
# Microsoft DNS Audits

This dashboard displays a comprehensive view of Microsoft DNS landscape, including traffic statistics.

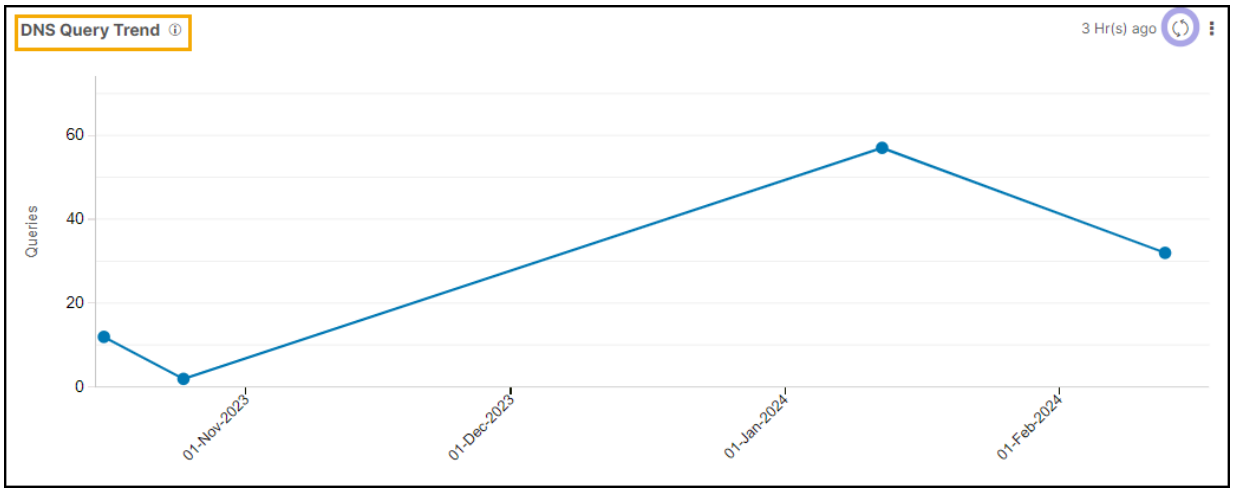



The following reports are available under the **Microsoft DNS_Audits** tab:

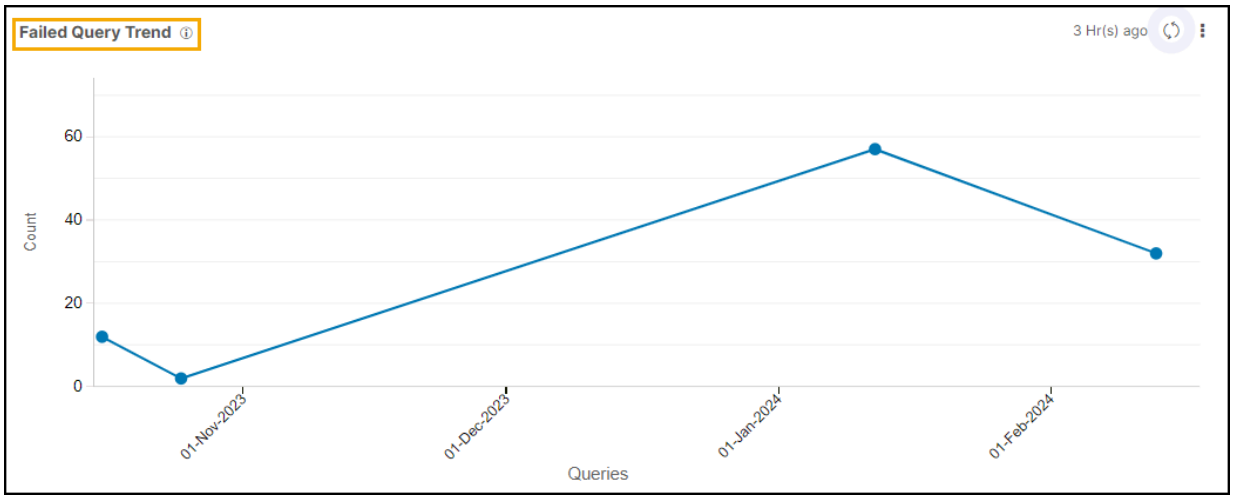
- **DNS Zones and Records Summary**: This metric displays the DNS Zones and Records Summary.
  - **Total DNS Zones**: This metric represent the total number of DNS Zones present across the Microsoft DNS servers managed in DDI+ platform.
  - **Total DNS Records**: This metric represent the total number of DNS records present across the Microsoft DNS servers managed in DDI+ platform.
  - **Total DNS Queries**: This metric represents the total number of DNS queries made on the Microsoft DNS servers managed in DDI+ platform.



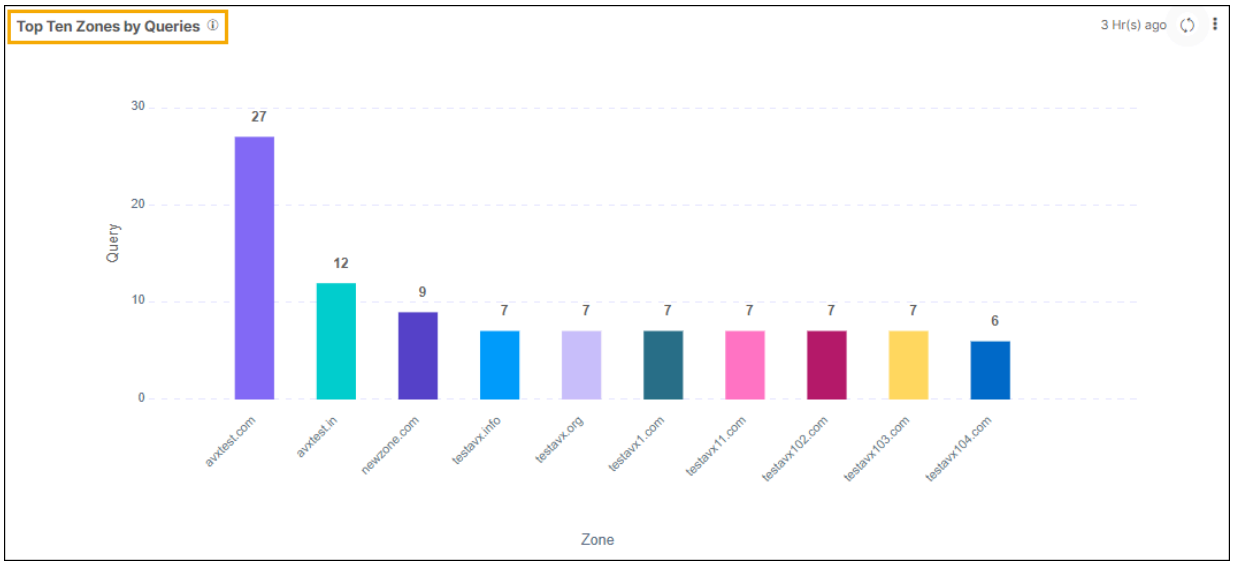

- **DNS Query Trend**: This report represents the daily DNS query trends.



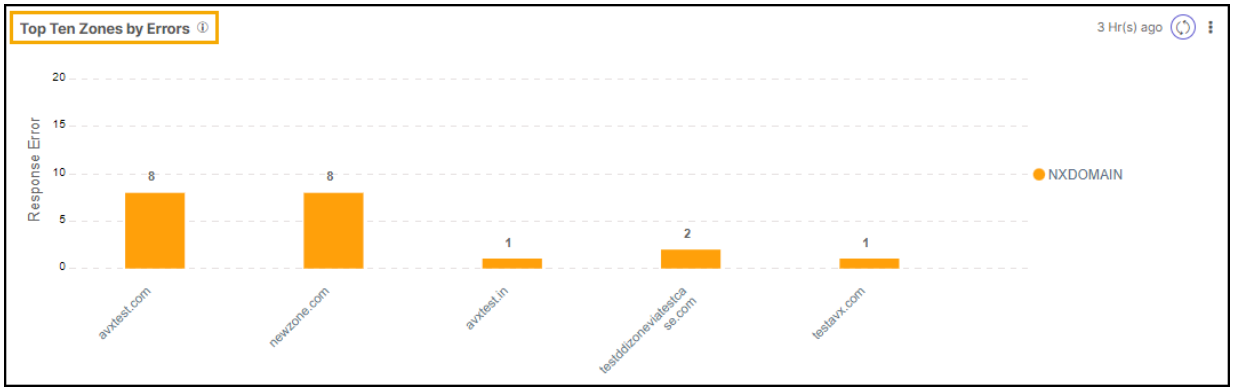

- **Failed Query Trend**: This reports represents the daily DNS failed query trends.



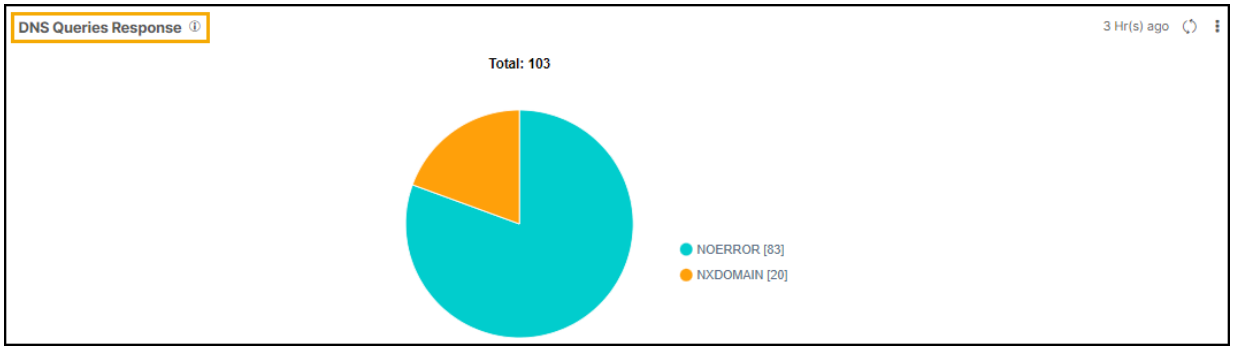

- **Top Ten Zones by Queries**: This bar chart illustrates the DNS Zones with the highest number of queries. The X-axis corresponds to the Zone names, while the Y-axis indicates the number of queries.



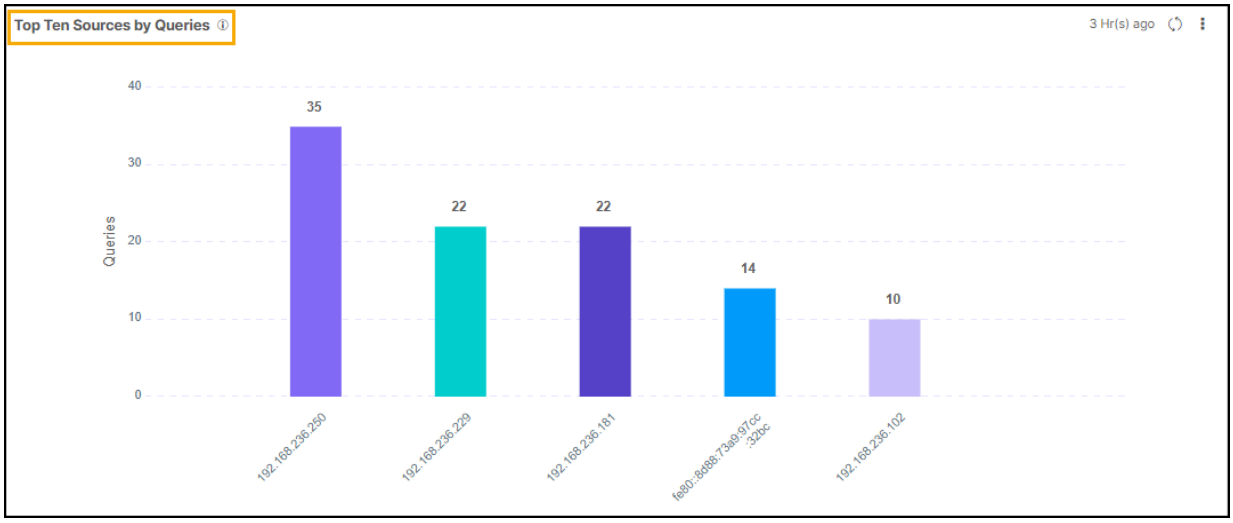

- **Top Ten Zones by Errors**: This bar chart depicts the top 10 DNS Zones with the highest number of query failures. The X-axis represents Zone names, and the Y-axis represents the number of failed queries.




- **DNS Queries Response**: This Pie chart represents total DNS queries response by error code type. such as NXDomain, SERVFAIL, and so on.



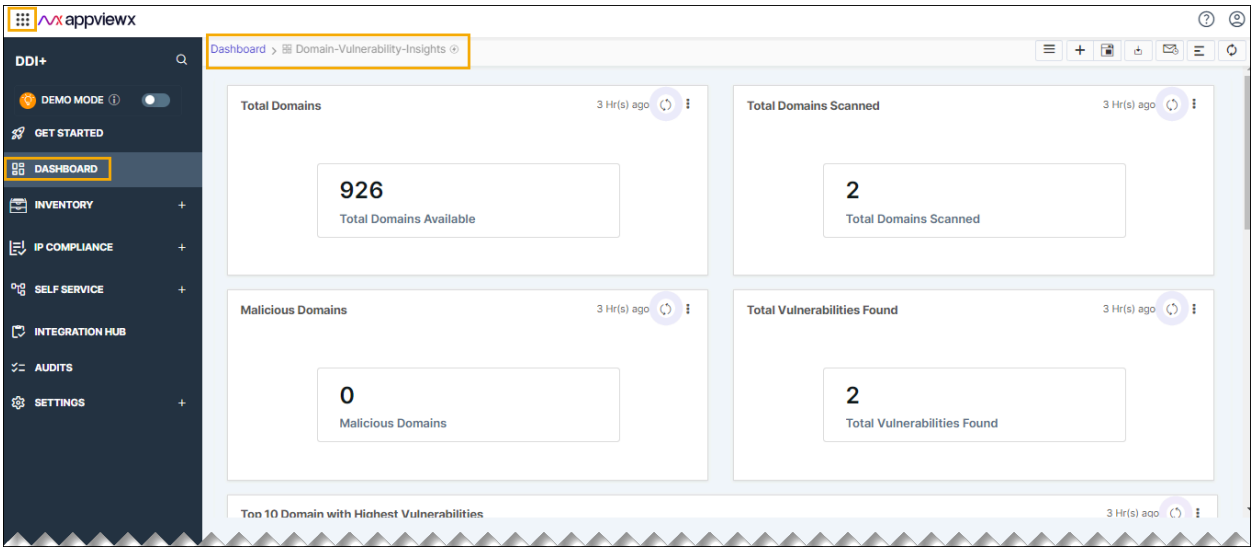
- **Top 10 Sources by Queries**: This bar chart illustrates the sources with the highest number of queries. The X-axis denotes the sources, while the Y-axis represents the corresponding number of queries made.




**Note:** You can click on the corresponding metric to view the detailed information.

## Domain Vulnerability Insights

The Domain Vulnerability Insights Dashboard offers a comprehensive overview of vulnerabilities across domains managed in DDI+ Platform. It provides insights into the total number of domains scanned for vulnerabilities, offering a detailed perspective on vulnerabilities within domains and their associated DNS records. This dashboard serves as a centralized tool for gaining valuable insights into the security posture of the managed domains.




The following reports are available under the **Domain Vulnerability Insights** tab:

- **Total Domains**: Total Domain Scanned provides the metrics of the total number of domains that are scanned from the domains.
- **Total Domains Scanned**: This metric displays the total number of domains scanned for the vulnerabilities.
- **Malicious Domains**: Provides a list of subdomains with CNAMEs redirecting to questionable websites. It specifically identifies instances where the content of the application in the CNAME includes malicious keywords.
- **Total Vulnerabilities Found**: This metric displays the total number of vulnerabilities found in the inventory.
- **Top 10 Domain with Highest Vulnerabilities**: This metric displays the top 10 domain with highest vulnerabilities in the inventory.
- **Domain Vulnerability by Types**: This bar chart illustrates vulnerabilities within domains and subdomains, categorized by various vulnerability scan types.

  The following vulnerability scans type:

  - **HTTPS/HTTP Scan:** This scan checks if the HTTP/HTTPS status is down for domains and associated subdomains.
  - **CNAME scan:** This vulnerability scan assesses vulnerabilities in CNAMEs associated with the domain. The scan includes checks for HTTP/HTTPS status, potential malicious content, and examines CNAMEs for standard response fingerprints susceptible to hijacking.
  - **MX Record Scan:** This scan involves checking domains for the presence of MXrecords. If the domains have MX records, the scan verifies whether the servers mentioned in the MX records are unreachable. If any servers are found to be unreachable, they are highlighted as vulnerable.

- **SPF Record Scan:** The SPF Record Scan involves multiple checks:
  - **Syntax Check:**The scan performs a syntax check on the SPF records.
  - **Reachability Check**: Verifies that all hosts mentioned in the SPF records are reachable.
  - **Invalid Directive:** Checks for invalid directives, such as instances where a domain is specified, but the MX record or the A record specified for that domain is invalid.
  - **Obsolete Include Directive**: Identifies and flags obsolete include directives, particularly when an invalid SPF for the domain specified in the existing record is detected.
- **DMARC Scan:** The scan verifies if the DMARC policy for the domain is set to "none." which potentially is a security concern.
- **NS Scan:** This involves verifying the reachability of the Name Servers (NS) associated with the domain through a ping test. The scan assesses the responsiveness of the NS servers, identifying any instances where they may be unreachable.
- **SOA Record Scan:** This scan aims to ensure that the SOA record adheres to specific criteria for optimal DNS configuration. Following are the criteria.
  - Ensures that the primary Name Server (NS) record specified in the SOA record is reachable.
  - Verifies that the refresh interval in the SOA record is set to a value greater than 3600 seconds.
  - Checks that the retry interval in the SOA record is set to a value greater than 900 seconds.
  - Ensures that the expiration time in the SOA record is set to a value greater than 604800 seconds.
  - Verifies that the Time-to-Live (TTL) value in the SOA record is set to a value greater than 300 seconds.

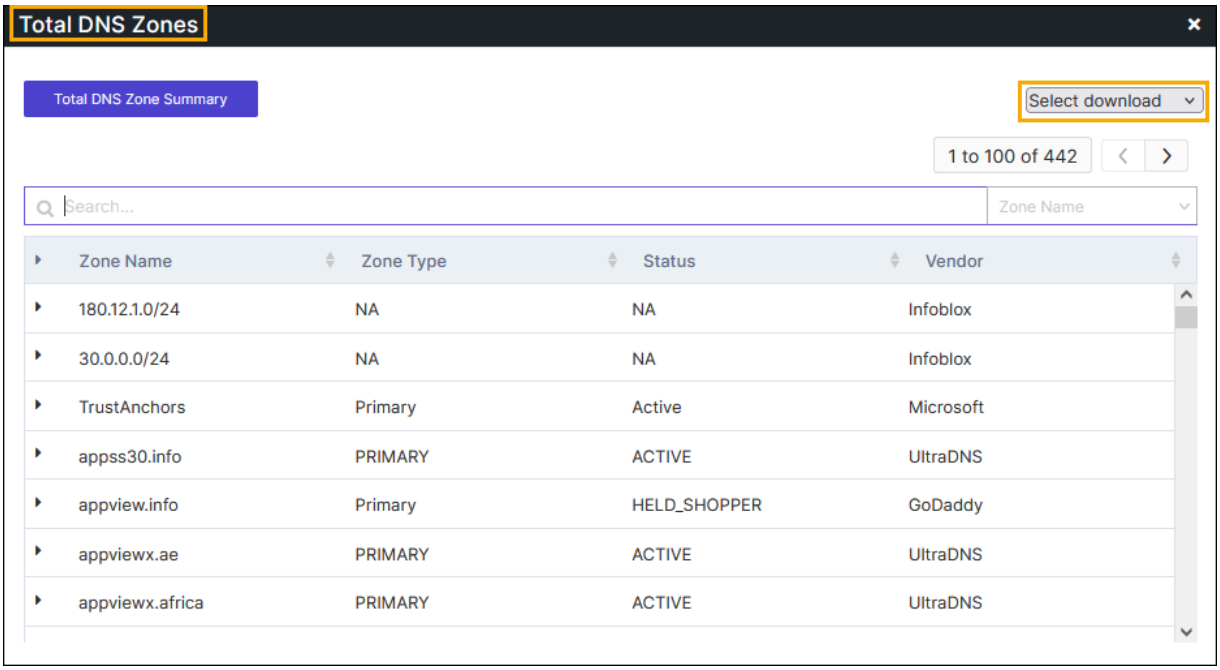
**Note:** You can click on the corresponding metric to view the detailed information.

## Downloading and Exporting the Dashboard Reports

To download/export the respective metrics, perform the following steps:

1. Go to **DDI+** > **Dashboard**, and then click on the desired metrics.

   The metrics is displayed with detailed information.



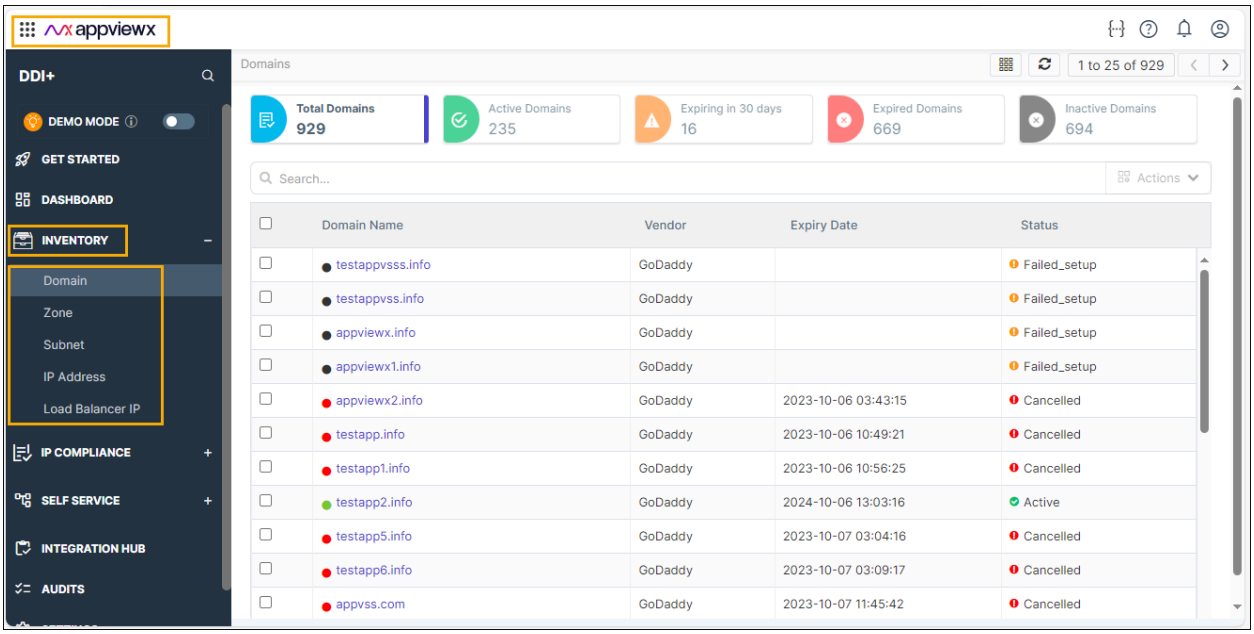

2. Click the (⋮) **Kebab** menu, and then click the **Select download** dropdown menu to download or export the file.

   The available options are:

   • Download as PDF
   • Export as Excel
   • Export as CSV.

## Inventory

The DDI+ inventory comprises a comprehensive list of System of Records, encompassing Domains, DNS Zones, Subnets, and IP addresses. It provides visibility into the correlations among DNS objects, establishing itself as the single source of truth for the DNS ecosystem.



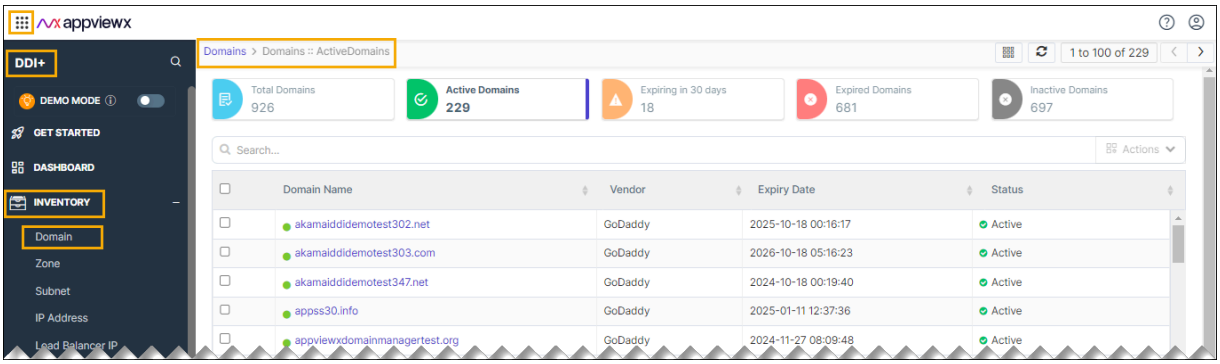

- Domains Inventory
- Zones Inventory
- Subnet Inventory
- IP Address Inventory
- Load Balancer IP Inventory

## Domains Inventory

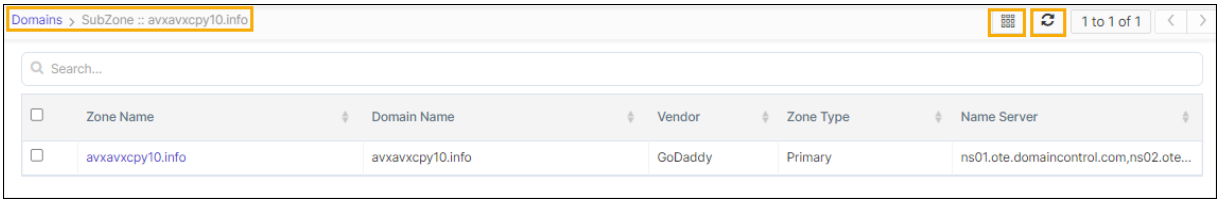
In the Domain Inventory section, users can access comprehensive details about all domains managed within the DDI platform. This includes vital information like domain names, configurations, and associated attributes, providing a detailed and organized overview of the entire domain portfolio. Additionally, this section offers the provision to view associated DNS Zones and records, even if managed by third-party DNS providers, offering a centralized view of domain ecosystem.

**Note:** Third-party DNS providers needs to be managed in DDI+ platform to view the DNS records and Zones.

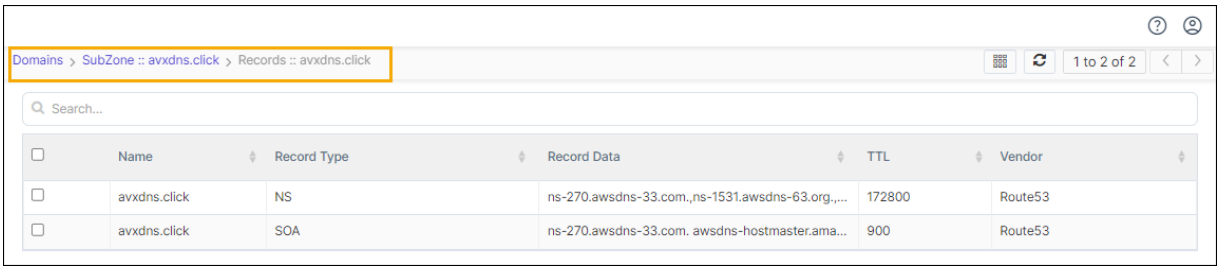
1. Go to **DDI+** > **Visibility**, and then click **Domain**.
   An inventory of all the domains is displayed with information about the vendor, status, expiry date, and so on.




2. Click on the domain name in the inventory to view the associated zone.




3. Click the Zone names to view the corresponding DNS records.




## Updating the Extensible Attributes for Domains

Extensible attributes are additional attributes that organizations may need to record as part of their domains. In the domain inventory, users can select a domain and update these extensible attributes.

1. Select the domain name from the list.
2. Click the actions table.
3. Choose **Update Attributes** from the options.

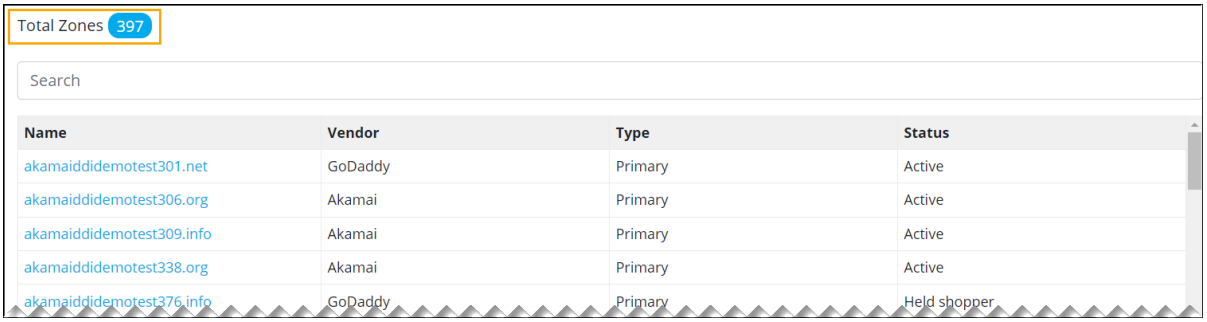
   A pop-up will appear with the attribute name and a field to enter the value. Click to here to configure the extensible attribute fields.
4. Enter the desired value, and then click **Save**.

   The attribute will be appended to the domain information in AppViewX.

## Zones Inventory

The zone inventory provides a comprehensive view of all zones and their associated DNS records distributed across a multi vendor DNS ecosystem.

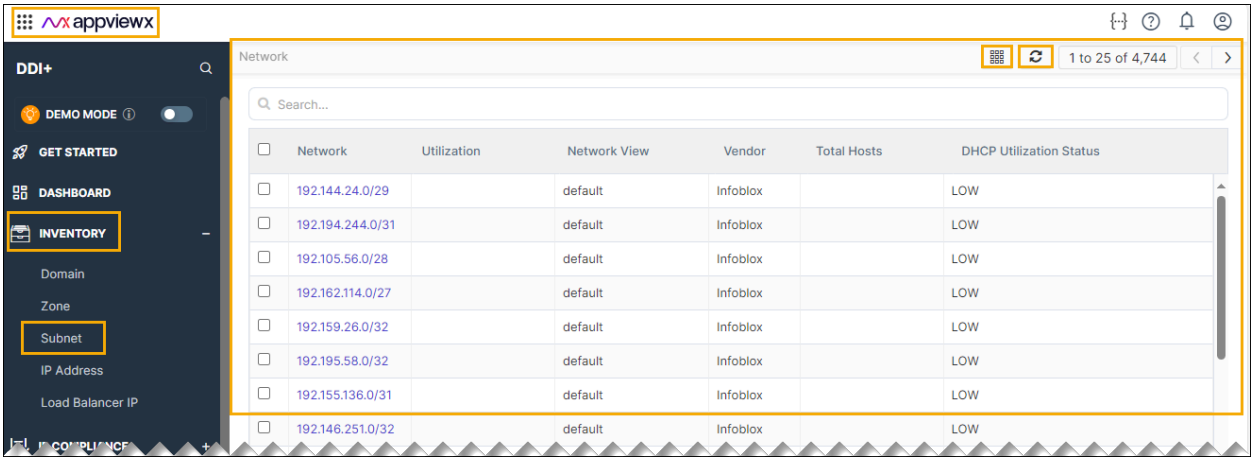
1. Go to **DDI+** > **Inventory**, and then click **Zone**.
   An inventory of all the zones managed across different DNS Vendors managed in DDI+ platform is displayed with information about the vendor, type of zone, and status.




2. For more information about a particular zone, click on the zone name from the list.
   You can view the corresponding DNS records.

## Subnet Inventory

The subnet inventory provides a comprehensive overview of all subnets present in the IPAM vendors . This includes detailed information on subnet configurations, associated attributes, and relevant network details.



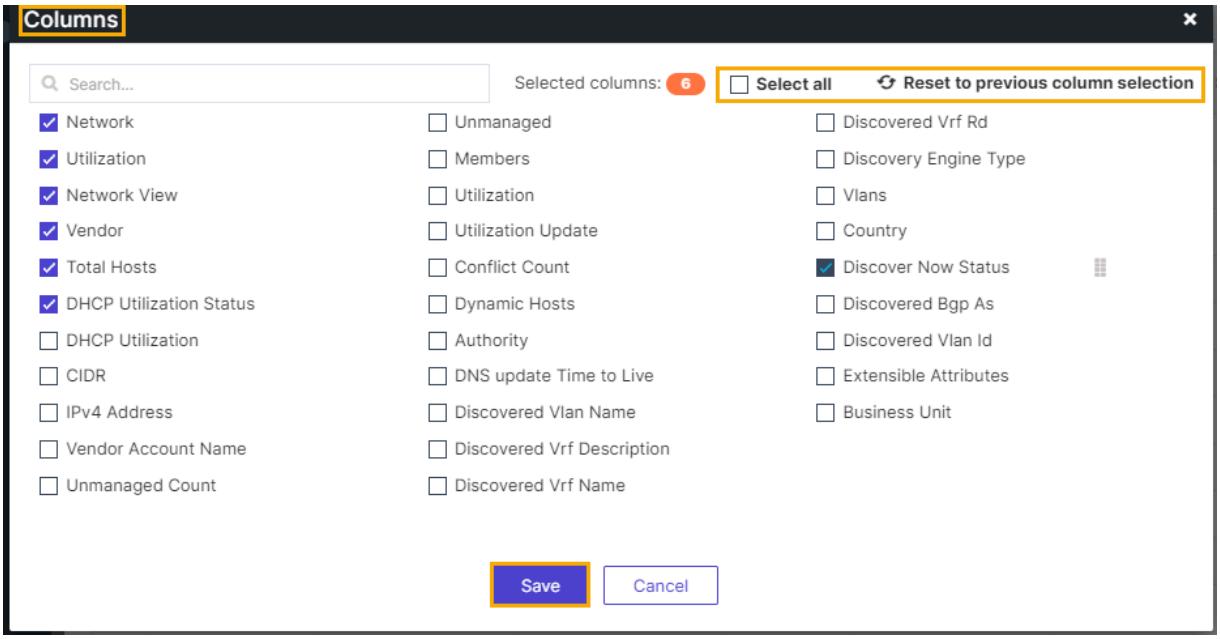
### IP - Subnet Inventory

1. Go to **DDI+** > **Inventory**, and then click **Subnet**.

   The IP address inventory page of the clicked subnet appears.

2. Click the  (**Columns**) icon to display to required columns on the subnet dashboard.

   The columns inventory page appears.

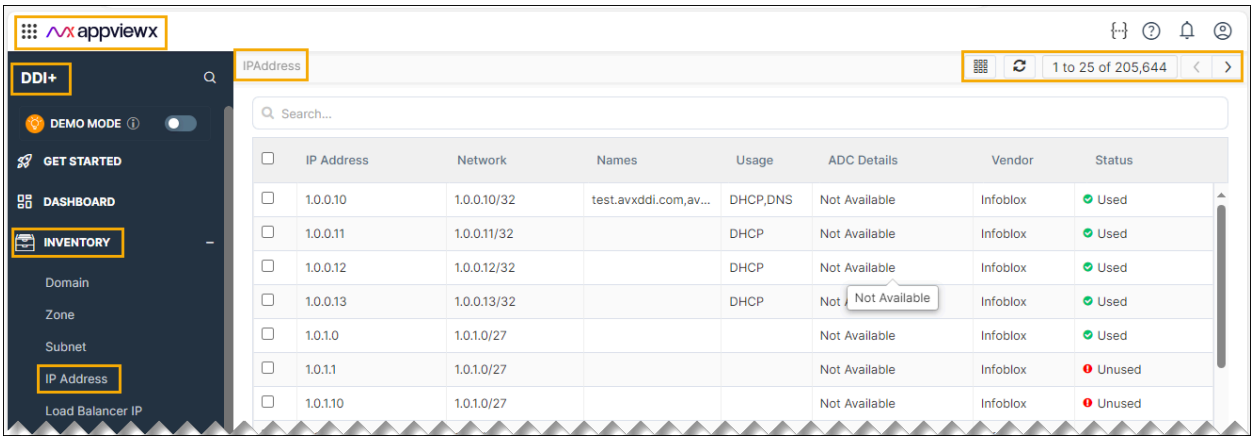



**Note:** You can use the search bar, and filter the search results by selecting the options from the dropdown.

a. Select the checkbox that to be displayed on the subnet inventory page.
b. Click **Save**.

## IP Address Inventory

The IP address inventory offers a thorough overview of all IP addresses within the network infrastructure. Users can access detailed information on IP configurations, associated attributes, and relevant network details across the IPAM, CMDB and Load Balancers. The IP Address Inventory provides a centralized view, enabling effective management and understanding of the entire IP address landscape across the network infrastructure.




1. Go to **DDI+** > **Inventory**, and then click **IP Address**.

   The **IP Address** inventory page appears.

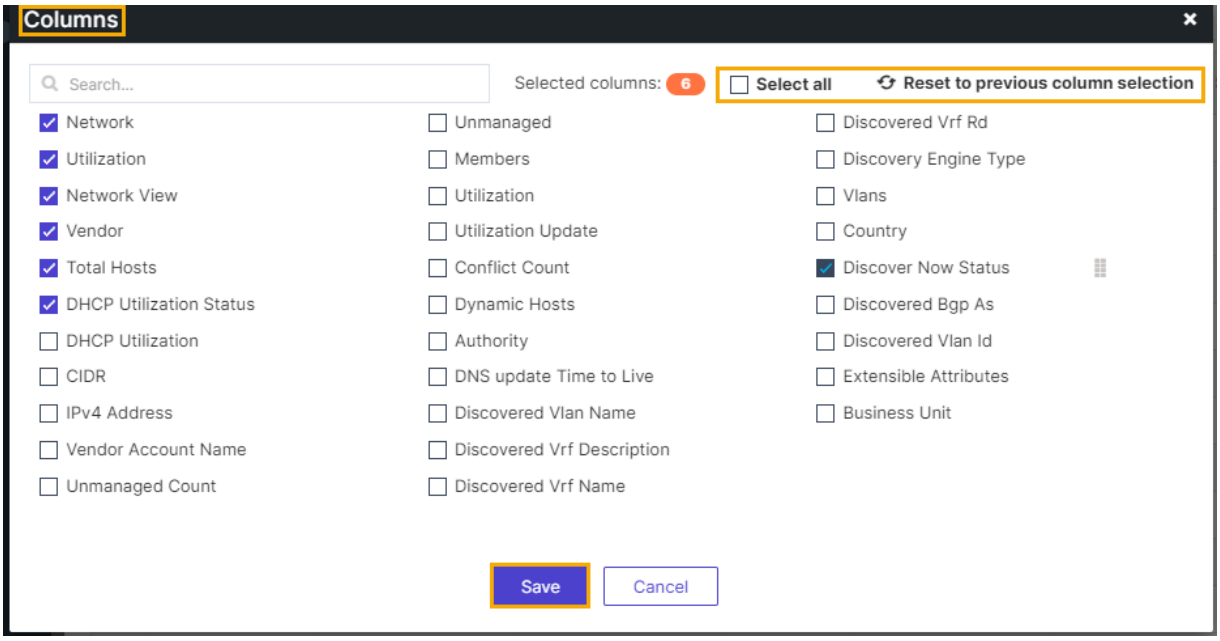
   **Note:** This inventory includes a column labeled **ADC Details**, indicating that the ADC details are available for each IP. This column comprises two values:

   - **Available**
   - **Not Available**

   If the **Available** is indicated, you can click on the hyperlink associated with the **Available** text to access and view the corresponding ADC details linked to the respective IP address.

2. Click the  (**Columns**) icon to display to required columns on the subnet dashboard.

   The columns inventory page appears.




**Note:**

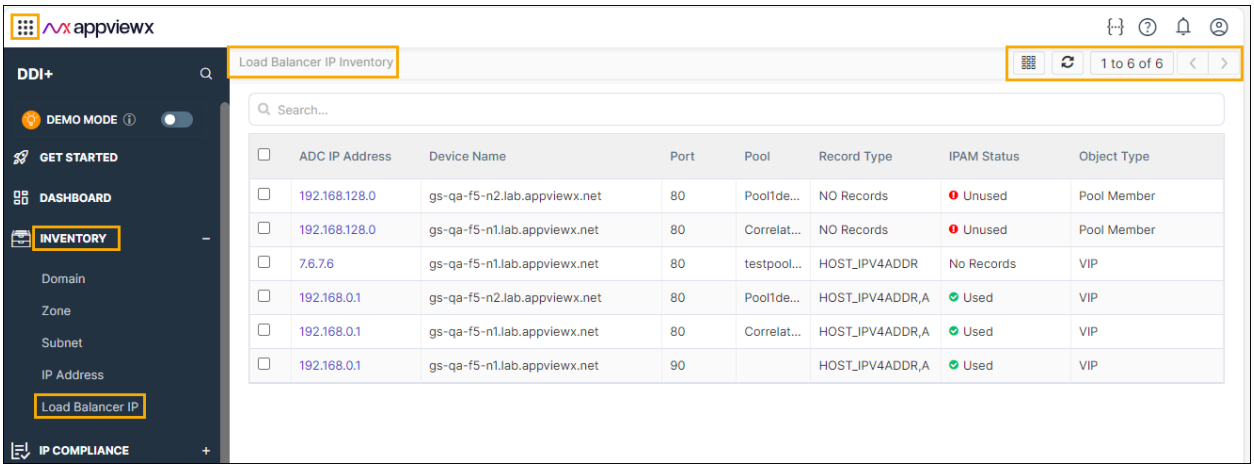
- You can use the search bar, and filter the search results by selecting the options from the dropdown.
- Column to be selected may contain the fileds from the CMDB configured in DDI+ platform.

a. Click the checkbox that to be displayed on the subnet inventory page.

b. Click **Save**.

## Load Balancer IP Inventory

The load balancer IP inventory presents a comprehensive view of all IP addresses associated with enterprise load balancers network infrastructure. It includes detailed information on configurations, attributes, and relevant load balancing details such as object types and associated objects such VIP to pool member association, IPAM status, and so on.

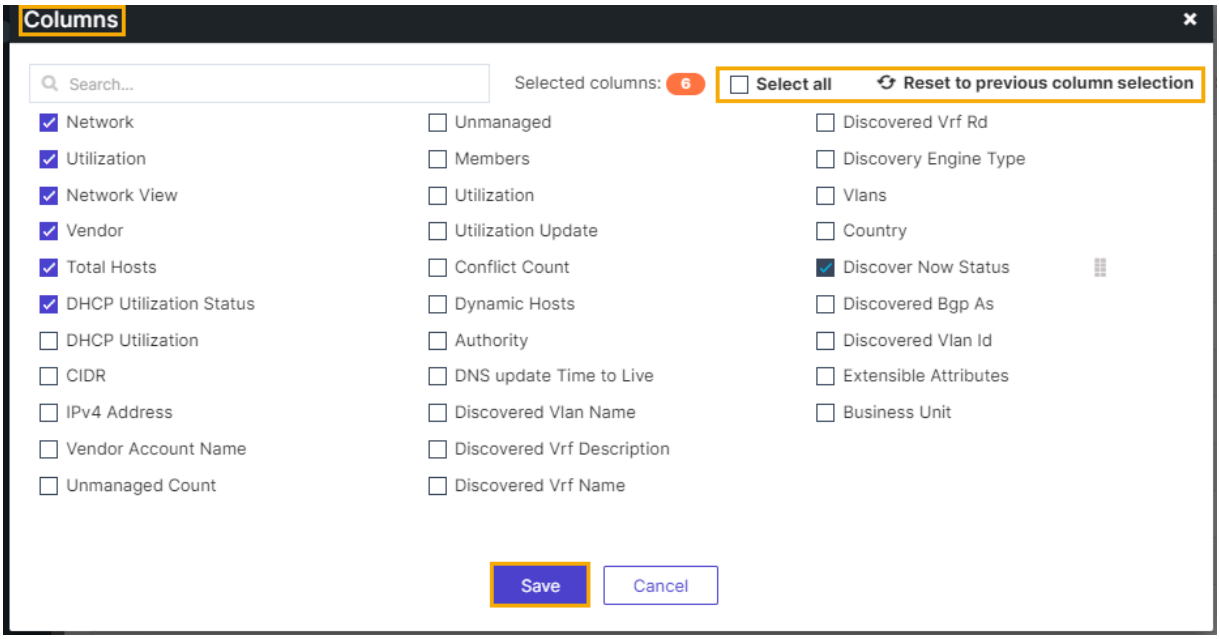



1. Go to **DDI+** > **Inventory**, and then click **Load Balancer IP**.

   The Load Balancer IP page appears.

2. Click the  (**Columns**) icon to display to required columns on the subnet dashboard.

   The columns inventory page appears.




**Note:** You can use the search bar, and filter the search results by selecting the options from the dropdown.

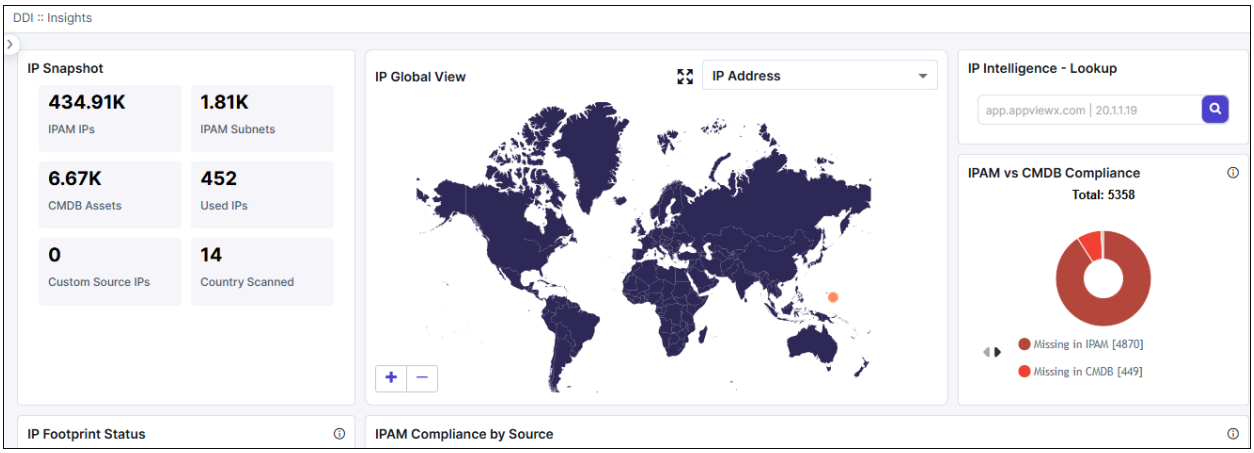
a. Click the checkbox that to be displayed on the subnet inventory page.
b. Click **Save**.

# IP Compliance

DDI+ empowers enterprises to gain comprehensive insights into the compliance of IP addresses distributed across IPAM, CMDB, and Load Balancers. By seamlessly integrating with IPAM and CMDB, it facilitates the correlation of IP addresses with CMDB assets, enabling the identification of ownership and detection of any discrepancies in IPAM and CMDB data. The solution ensures synchronization between CMDB and IPAM, highlighting IPs lacking ownership information and providing visibility into potential violations between load balancer, IPAM, and ADC IP addresses. Additionally it provides app-centric correlation across IPAM, CMDB, Load Balancers and Firewalls.

**IP Compliance Features**:

- **IP Compliance Dashboard**
  - Provides end-to-end visibility into the IP estate and identifies any violations across IPAM, CMDB, and Load Balancers.
  - Comprehensive overview of IP compliance status.
- **IP Search**
  - Enables users to search for IP addresses or FQDNs, providing application-centric visibility across IPAM, CMDB, Load Balancers, and firewalls.
  - Quick and targeted access to IP-related information.
- **IP Hygiene**
  - Ensures compliance across CMDB and IPAM by allowing users to update information through a self-service form, streamlining the process.
  - Efficient maintenance of accurate and compliant IP information.




## Configuring IP Compliance

To configure compliance reports and build the compliance dashboard, the following steps needs to be performed:

- **Integrate CMDB**: Configure the DDI+ platform with the tables in CMDB from which CMDB IP asset information needs to be synced.
- **Integrate IPAM**: Onboard the IPAM vendor and select the pre-configured CMDB settings in AppViewX.
- **Integrate ADC**: Onboard ADC vendors in AppViewX to obtain ADC IP correlation and identify compliance violations.
- **Integrate Firewall**: Onboard Firewall vendors in AppViewX to obtain firewall NAT IP correlation. Identify Public to Private translation and view translate IP meta data and correlation.

- Summary
- IP Search
- Hygiene

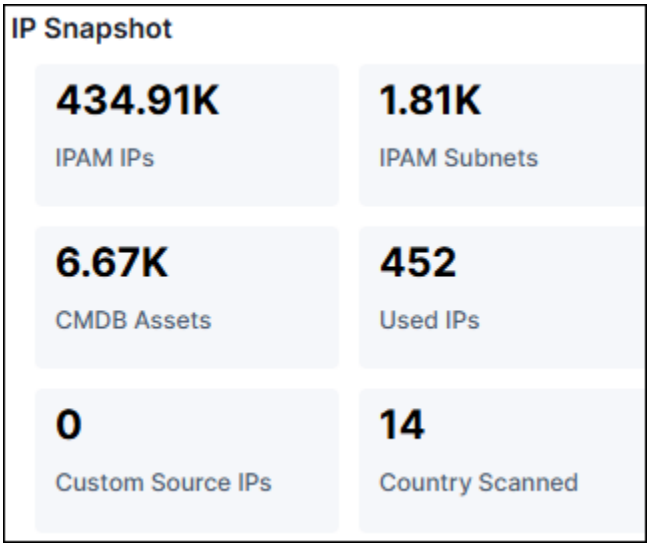
## Summary

The IP compliance summary dashboard provides a overview of IP address landscape and compliance status with CMDB and Load balancing configuration.

The following reports are available under the **IP Compliance** > **Summary** tab:

## IP Snapshot

The IP Snapshot dashboard provides a summarized view of IP address management (IPAM) data. It gives insights into IP address allocations, compliance status, and asset inventory, assisting network and security teams with visibility and decision-making.

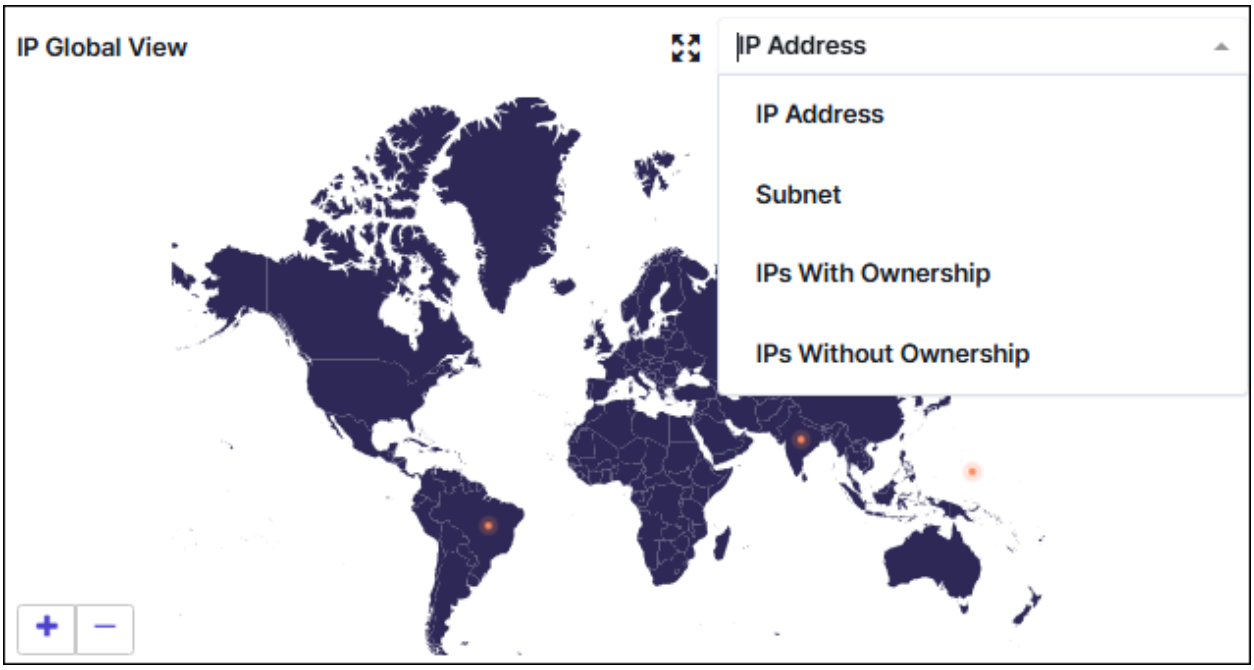



Click on the parameter to open a popup with detailed information about the IPs.

| Metric | Description |
|---|---|
| **IPAM IPs** | Total number of IP addresses managed within the IP Address Management (IPAM) system. |
| **IPAM Subnets** | The number of subnets registered in the IPAM database. |
| **CMDB Assets** | Number of assets recorded in the Configuration Management Database (CMDB) that are associated with IPs. |
| **Used IPs** | IPs actively used across your environment. This includes systems currently online and assigned an IP. |
| **Custom Source IPs** | Number of IPs sourced from external or custom data feeds not originating from standard IPAM or CMDB. |
| **Country Scanned** | The number of distinct countries from which IPs have been scanned or detected. |

## IP Global View

**IP Global View** which is used to monitor IP addresses geographically to detect unusual IP activity in specific regions, and Asset Management to track owned IP blocks.




- **Global Map View:** Displays the entire world, highlighting locations where IP addresses are in use or monitored.

> **Note:** Zoom Controls: **+** and **-** allow zooming in and out for more detailed views of specific regions.

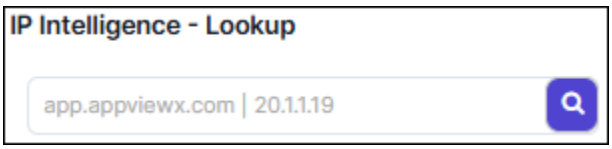
> **Note:** To expand the screen, select the expand icon.

- **Dropdown Menu** (Top-Right) it allows to filter and view the data based on set parameters:
  - **IP Address:** Displays individual IPs on the map.
  - **Subnet:** Groups IPs by subnet and displays aggregated data.
  - **IPs With Ownership:** Displays the list of IPs that are registered or assigned to specific organizations or users.
  - **IPs Without Ownership:** Displays unassigned or publicly accessible IPs.

  The selected option from the dropdown is displayed on the map as red dots. Clicking the dot opens a popup with detailed information about the IPs in that region/country.

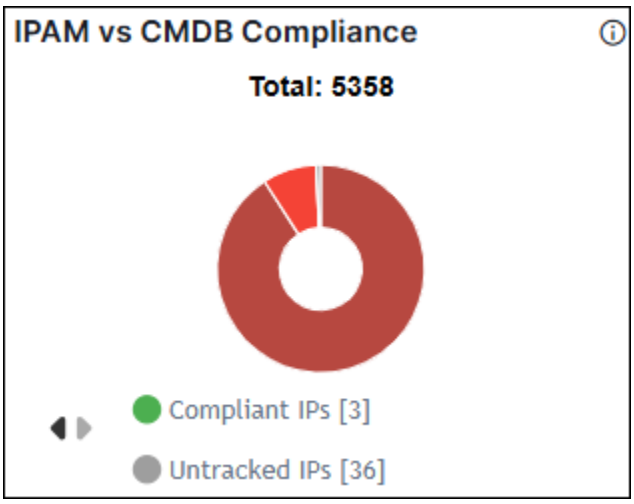
## IP Intelligence - Lookup

The IP Search page allows users to search for an IP address or FQDN, providing Appcentric visibility and correlation across IPAM, Load balancers, and Firewalls. Users have the flexibility to search for both private and public IP addresses or FQDNs. To know more details, click here.




## IPAM vs CMDB Compliance

This report highlights IP compliance status between IPAM and CMDB:




Click compliance chart to view the required IP report list.

- **Compliant IPs**: IP is used in both IPAM and CMDB.
- **Missing in CMDB**: IP Used in IPAM but not present CMDB.
- **Missing in IPAM**: IP is in CMDB but not used in IPAM.
- **Untracked IPs**: IP is unused in both IPAM and CMDB but present in other source (e.g., ADC, CMDB, L2/L3 devices, custom sources).

Clicking on the chart opens a popup window that includes:

1. **Detailed IP Address List**: View individual compliant, Untracked IPs, Missing in IPAM, and Missing in CMDB along with associated metadata.
2. **Search bar**: Quickly filter specific IP by address, compliance status, or associated source.
3. **Download icon**: Export the list in CSV or Excel format for offline analysis.

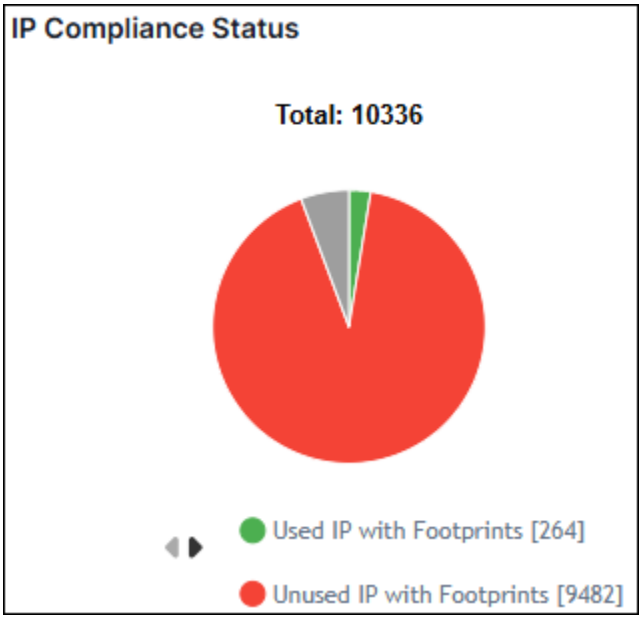
- For large reports (e.g., over 500K rows), the download is automatically split into multiple files, each containing up to 300K rows.

> **Note:** A zip file is downloaded with the report name and contains multiple files.

4. **Email icon**: Directly send the IP compliance report to specified email addresses as attachment.

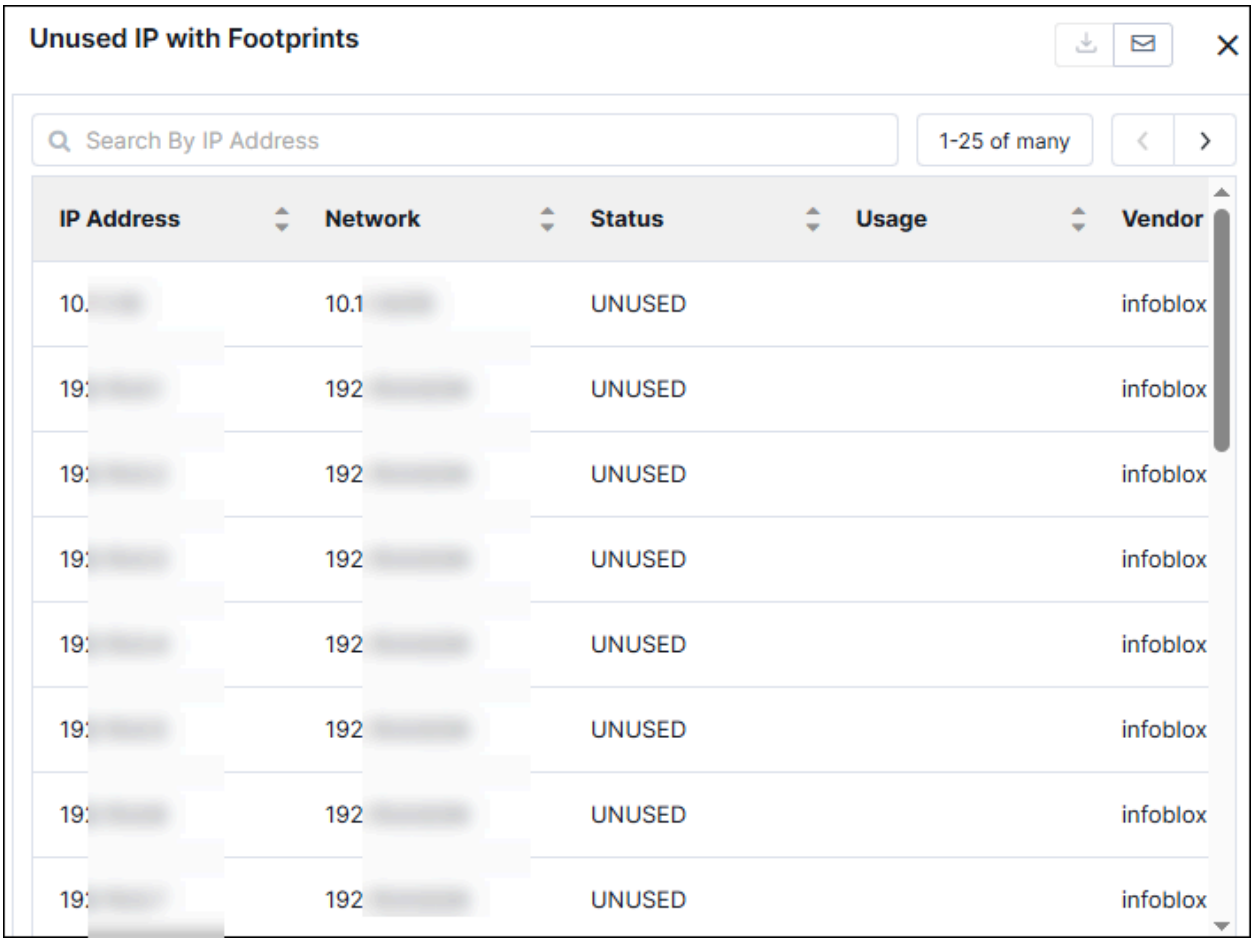
### IP Compliance Status

This report provides an overview of IP compliance against sources:




- **Used IP with Footprints**: IP used in IPAM and is found in at least one source (ADC, CMDB, L2/L3 devices, or custom sources).
- **Unused IP with Footprints**: IP unused in IPAM but has been discovered in other sources.
- **Used IP with No Footprints**: IP exists in IPAM but has no footprint in any discovered sources.

Clicking on the chart opens a popup window that includes:

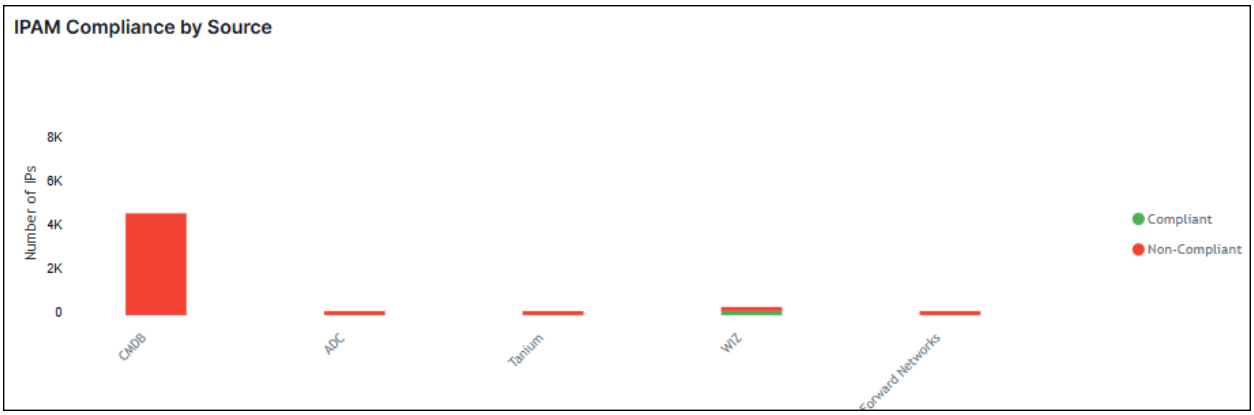



1. **Detailed IP List**: View individual **Used IP with Footprints**, **Unused IP with Footprints**, and **Used IP with No Footprints** along with associated metadata.
2. **Search bar**: Quickly filter specific IP by address, compliance status, or associated source.
3. **Download icon**: Export the list in CSV or Excel format for offline analysis.
   - For large reports (e.g., over 500K rows), the download is automatically split into multiple files, each containing up to 300K rows.

   **Note:** A zip file is downloaded with the report name and contains multiple files.
4. **Email icon**: Directly send the IP compliance report to specified email addresses as attachment.

## IPAM Compliance by Sources

This report compares IP compliance across different discovery sources (e.g., ADC, CMDB, L2/L3 devices, custom sources) against IPAM's used data. It categorizes IPs as:




- **Compliant:** IP used in IPAM and found in the respective source.
- **Non-Compliant:** IP is not used in IPAM but exists in the respective source.

Clicking on the chart opens a popup window that includes:

1. **Detailed IP List**: View individual compliant or non-compliant along with associated metadata.
2. **Search bar**: Quickly filter specific IP by address, compliance status, or associated source.
3. **Download icon**: Export the list in CSV or Excel format for offline analysis.
   - For large reports (e.g., over 500K rows), the download is automatically split into multiple files, each containing up to 300K rows.

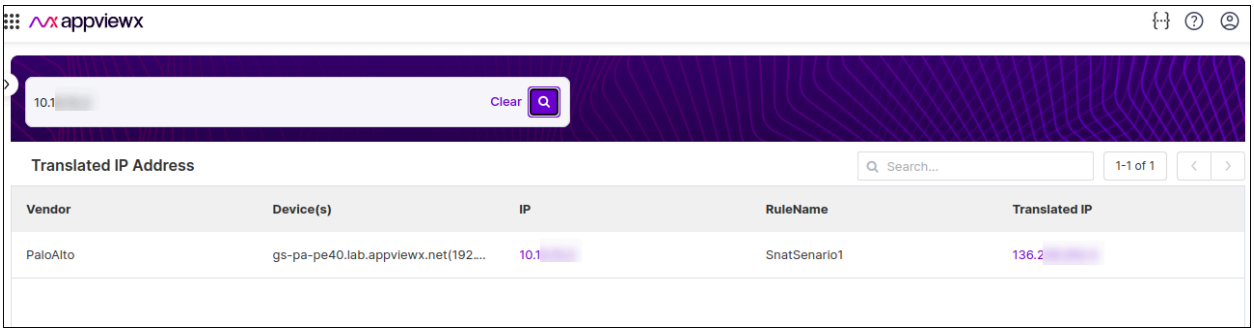
   **Note:** A zip file is downloaded with the report name and contains multiple files.

4. **Email icon**: Directly send the IP compliance report to specified email addresses.

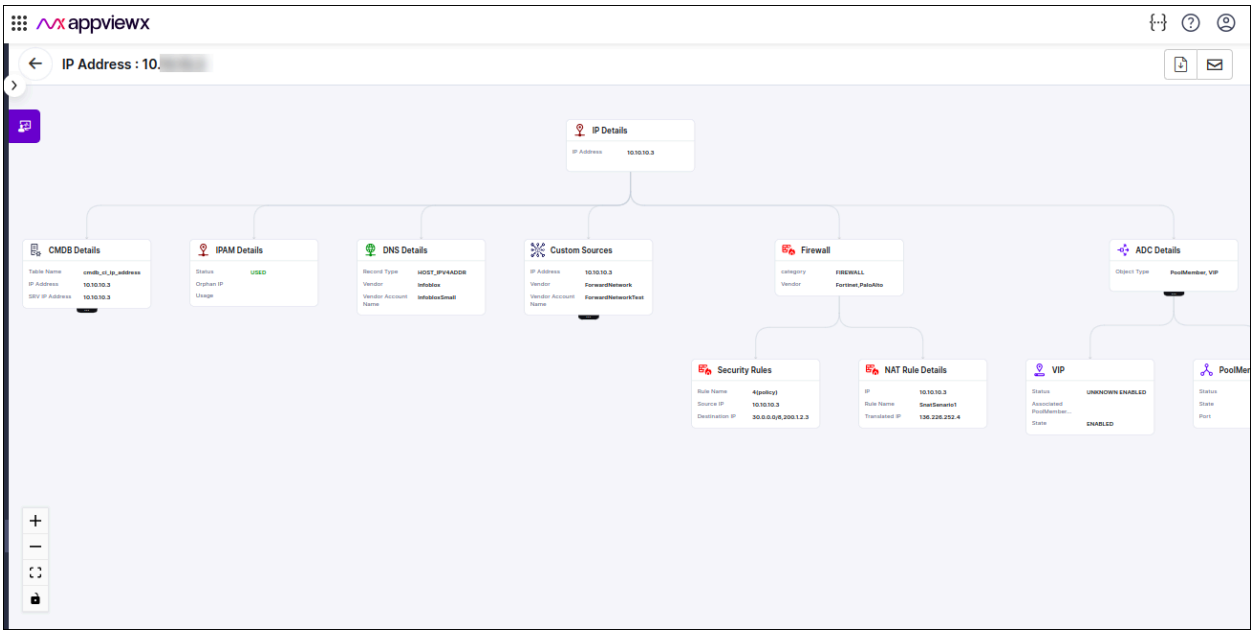
## IP Search

The IP Search page allows users to search for an IP address or FQDN, providing Appcentric visibility and correlation across IPAM, Load balancers, and Firewalls. Users have the flexibility to search for both private and public IP addresses or FQDNs.


When a public IP is searched, the system presents a grid displaying any Network Address Translation (NAT) rules associated with the translation to a private IP. Users can explore these NATTED rules and view correlations with private IP addresses in a hierarchical format. In the case of a private IP search, users will be directly presented with the hierarchical view.

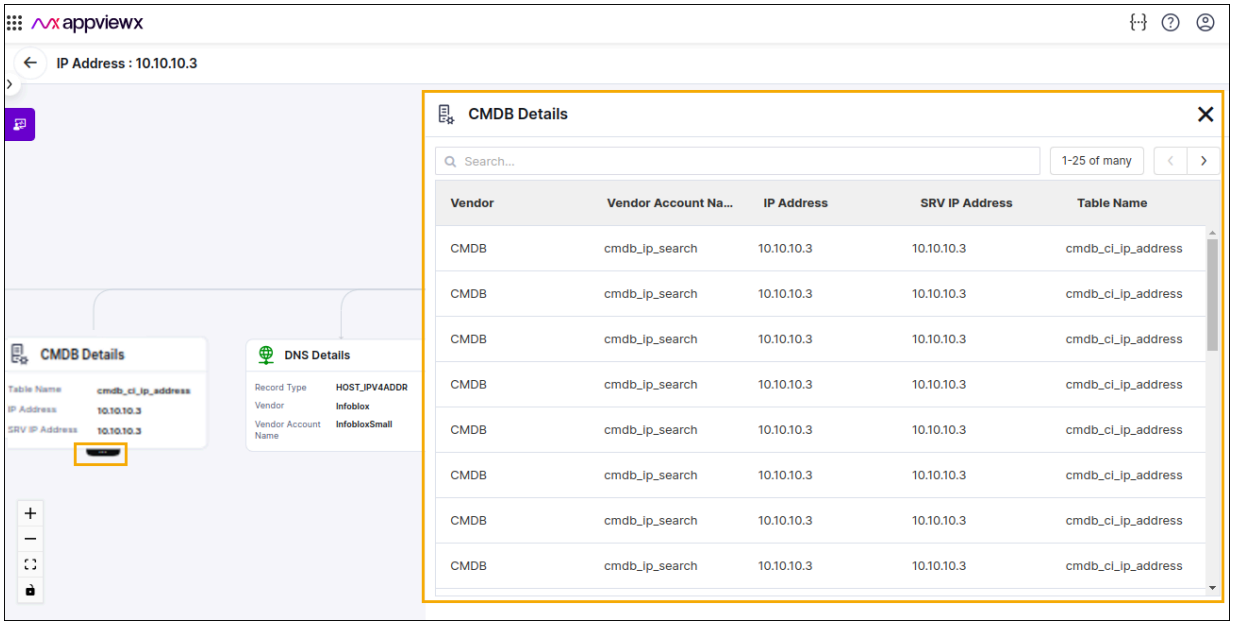



Once the IP users clicks the search icon or view button incase of NAT IP, a correlation of all IP addresses will be shown in a hierarchical view as below.




In the hierarchical view, users can:

- Search asynchronously across multiple data endpoints or sources.
- View a summary of the sources.
- If a source contains multiple IP addresses, click the view more option associated with the node to view the detailed tables for each source.



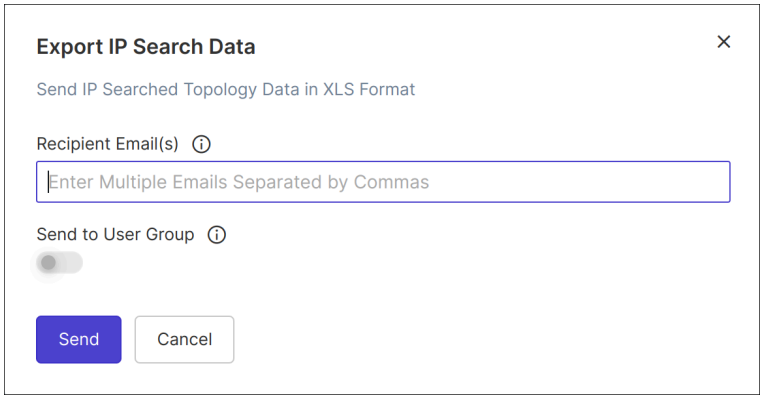

- Download the IP/FQDN details in the Excel format by clicking the download icon located in the upper right corner. The Excel file will be downloaded to the default download folder.

- Send the IP/FQDN details through email as an attachment to the email addresses or the user groups.

  To send the IP details through email:

  1. Within the IP Search page, click the email icon located in the upper right corner.

     The **Export IP Search Data** window opens.



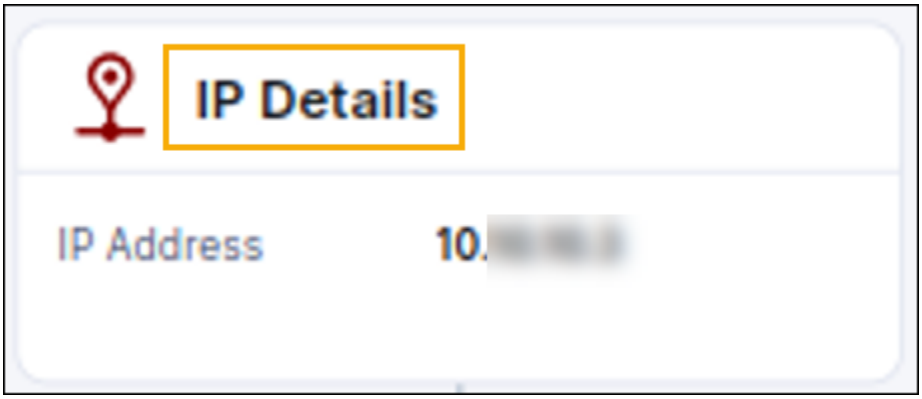

  2. In the **Recipient Email(s)** field, enter the email addresses with comma separated.
  3. If required to send the email to the user group, enable the **Send to User Group** toggle button, and then select the user group(s) from the **User Group** dropdown option.
  4. Click **Send**.

     The email will be sent to the recipients with the IP details attachment.

Users can click on each node to view the corresponding details such as IPAM, DNS, CMDB, Load balancer, Firewall details.

**IP Details**

IP Details node represents the IP address details retrieved from IPAM , encompassing associated information such as subnets, status, device name, etc. Click on the node to view more details.

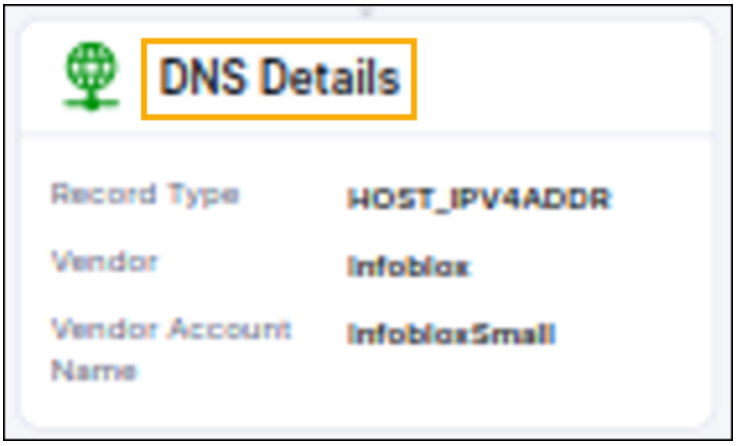



**IP Address**

This node represents the IP address searched.


**DNS Details**

The DNS Details node represents associated DNS record details for the respective IP address. Users can click on the node to access additional details.




**CMDB Assets**

CMDB details represent all the IP asset information retrieved from the CMDB. Click on the node to view more information.


**ADC Details**

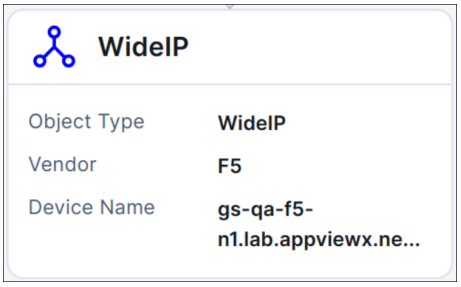
This node denotes the type of ADC objects linked to the searched IP address. For instance, if the searched IP address functions as WideIP, GTM Pool member, Pool member, or VIP object, the "Object Type" will display as "WideIP, GTM Pool member, Pool Member, VIP." The child of this node contains additional details specific to either the VIP or Pool member.


**VIP Node**

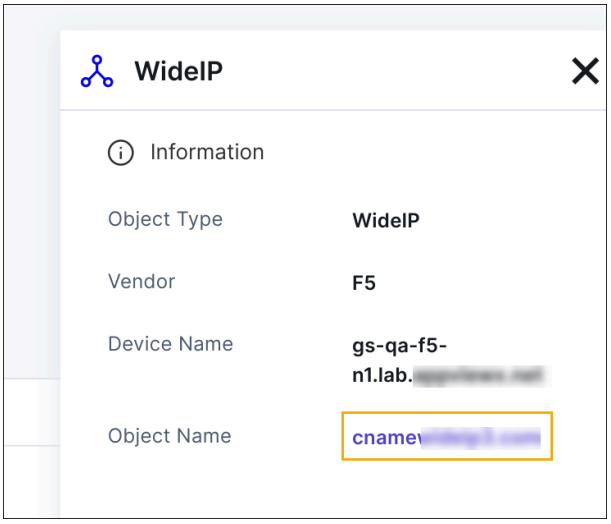
This node signifies details about the VIP associated with the IP, providing additional information specific to the respective VIP upon clicking. Additionally, this node may have one child representing all the Pool members associated with the VIP.


**WideIP**

This node signifies details about the WideIPs associated with the IP, providing additional information specific to the respective WideIP upon clicking. Additionally, this node may have one child representing all the GTM Pool members associated with the WideIP.




If this associated WideIP is CNAME, then the object name is provided as URL, which redirects to the FQDN in the IP search.




**Firewall Details**

This node represents the if there is any Firewall NAT rule association with the searched IP address. The child node represents the details of the Firewall NAT rules as shown below.

1. Go to **DDI+** > **IP Compliance**, and then click **IP Search**.

   The IP Search page appears.

2. Select the **IP Address** or **Domain/FQDN** from the dropdown that you want to search.
3. Enter the value <IP Address or Domain name> in the field.
4. Click **Search**.

   The search result appears on the page.

**L2/L3**

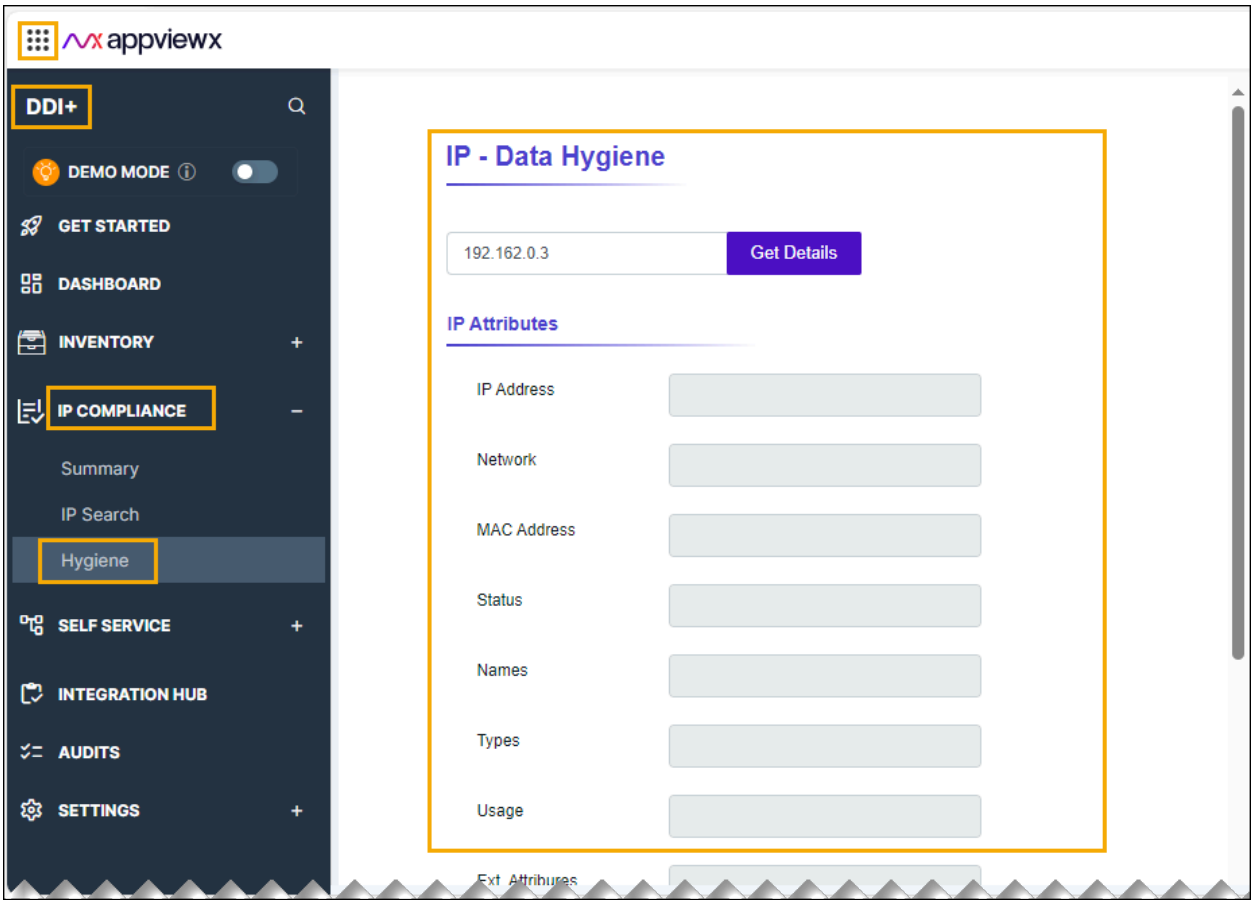
This node signifies details about the ARP or VRF associated with the IP, providing additional information specific to the respective ARP or VRF upon clicking. Additionally, this node specifies the details of the interfaces VLANs if configured within IP.


## Hygiene

IP Compliance Data Hygiene refers to the status and cleanliness of IP address data within the network infrastructure. It involves ensuring that all IP addresses are properly allocated, organized, and compliant with the network's configuration standards and policies.

Ensure compliance for IP addresses across IPAM, DNS, and CMDB. Utilize this Self-Service form to:

The following reports are available under the **Hygiene** tab:




1. Go to **DDI+** > **IP Compliance**, and then click **Hygiene**.

   The Hygiene page appears.

2. Ensure compliance for IP addresses across IPAM, DNS, and CMDB. Utilize this Self-Service form to:
   a. Enter an IP Address and search for details across DDI and CMDB.
   b. View DNS and IPAM details.
   c. Create IP reservations if no reservation is found.
   d. Create DNS records.
   e. Update CMDB information.

## Self Service

This section offers a comprehensive catalog for provisioning DNS and domain services across multiple vendors. Users can leverage self-service functionalities and automation tools to efficiently manage the entire lifecycle of domains and DNS configurations, ensuring a streamlined automation process.

## Domain Lifecycle



## Register a Domain

To register a domain follow the below steps.

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Register Domain**.
   The workflow execution page is displayed with the workflow inputs requested at the first stage.

   **Note:** You can navigate back to the **DDI+** home page, by clicking (**Home**) icon from the top left corner of the screen.

2. In the Info field, read the workflow usage instructions.
3. In the **Requester Details** section, enter the **Requester Name**, **Requester Email Address**, and **Team DL** in the respective field.

   **Note:** Multiple email addresses must be entered as comma-separated values. The field information for the first two fields will be fetched automatically from the logged in user information.

4. In the **Domain Search** section, enter the **Domain Registrar**, **Domain Account**, and **Domain Name** that you want to register.

5. To check if the requested domain name is available, click **Check Domain Availability**.
   - If the domain name is already registered, the following header notification is displayed on the top of your screen in red:


   - If the domain name is available, the following header notification is displayed on the top of your screen in green and the remaining fields in the Domain Search section are auto-populated:

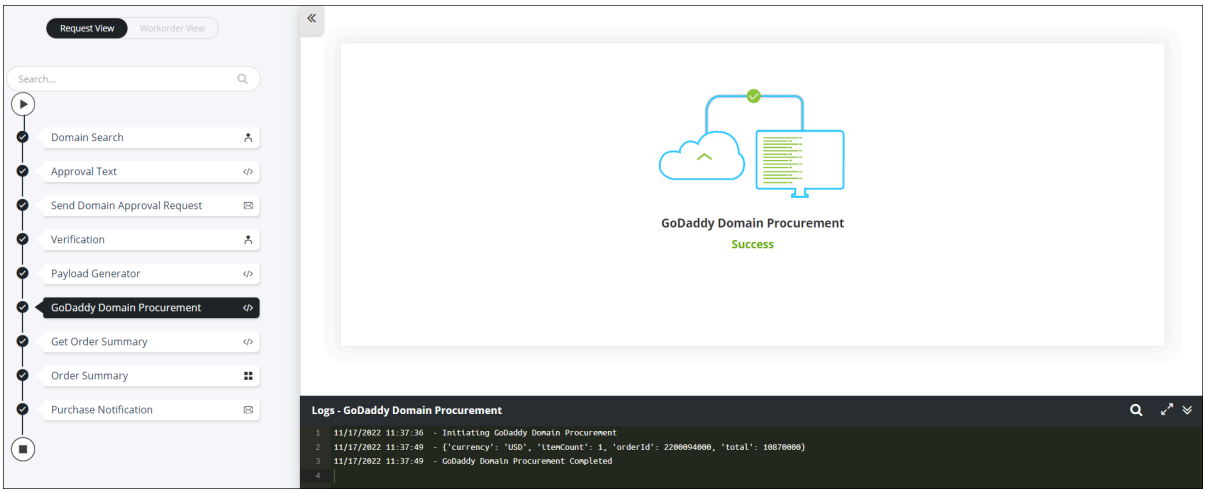

   The following table describes the other fields in this section:

| Field | Description |
|---|---|
| ***Domain Price (USD)** | Displays the price (per annum) for registering the domain. |
| ***Auto Renewal** | Select Off or On depending on whether you want to enable Auto Renewal.<br>**Note:** If Auto Renewal field selection is **On**, the domain name is automatically renewed when it is about to expire. If the selection is **Off**, an expiry notification will be sent to the approver to renew the domain name. |
| ***Validity Period Years)** | By default, this value is auto-populated as 1 year. You can change the value for up to 10 years. |
| ***NameServer Selection** | Select the method for NameServer Selection:<br>• **Registrar's Default**: A default NameServer is provided by the Registrar.<br>• **Auto**: NameServer will be fetched from the values configured during the Registrar integration.<br>• **Manual**: You can manually add custom NameServers. |
| **: Mandatory fields* | |

6. In the **Additional Domain Info** section, enter or select the required field information.

| Field | Description |
|---|---|
| **Business Unit** | Select the business unit as configured during the Registrar integration. |
| **Tags** | Enter tags to be associated with the domain (if required). |
| **Comments** | Enter any comments (if required). |

7. Click **Submit**.
   At the **Verification** stage of the workflow execution, an email for domain name approval is sent to the approver. Once the approver approves the request, the domain is procured.




8. To view the order details, go to the **Order Summary** stage of workflow execution.
9. To download a copy of the order summary, from the top right corner of the screen click  (**Download**) icon.

## Provisioning DNS Records

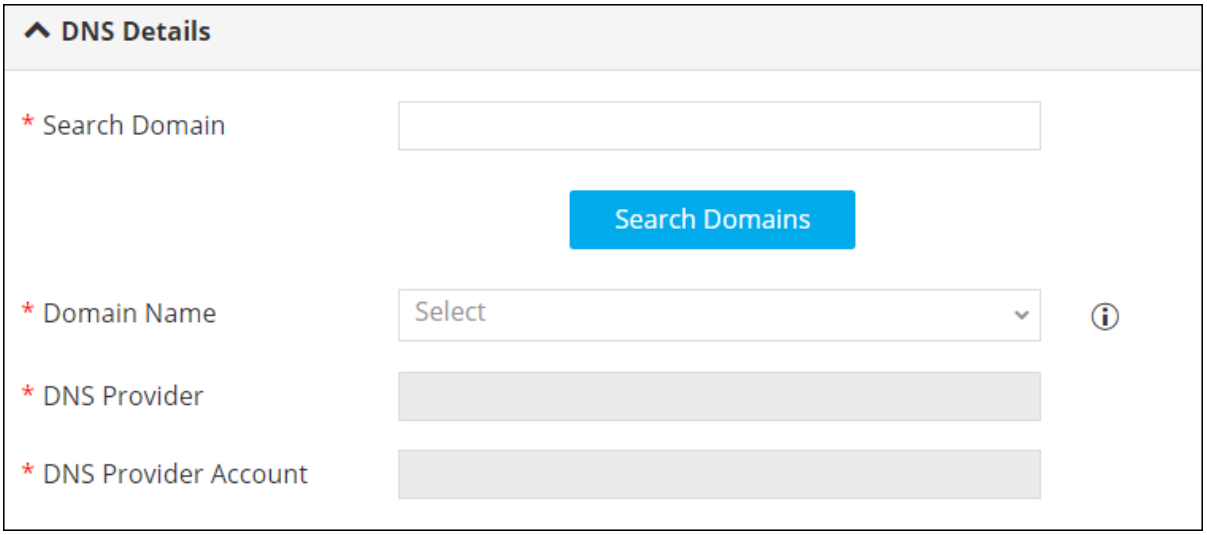
DNS records provide information about domains such as IP address(es) associated with that domain, handling requests for the domain, and so on.

To add DNS records to your hosted zones:

1. From the **Domain Lifecycle** section, click **Add DNS Records**.
   The workflow execution page is displayed in a new tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent.

**Note:** Multiple email addresses must be entered as comma-separated values. The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, in the **Search Domain** field, enter search text/keywords for searching domains.
4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields in the **DNS Details** section.




The following table describes the field information required here:

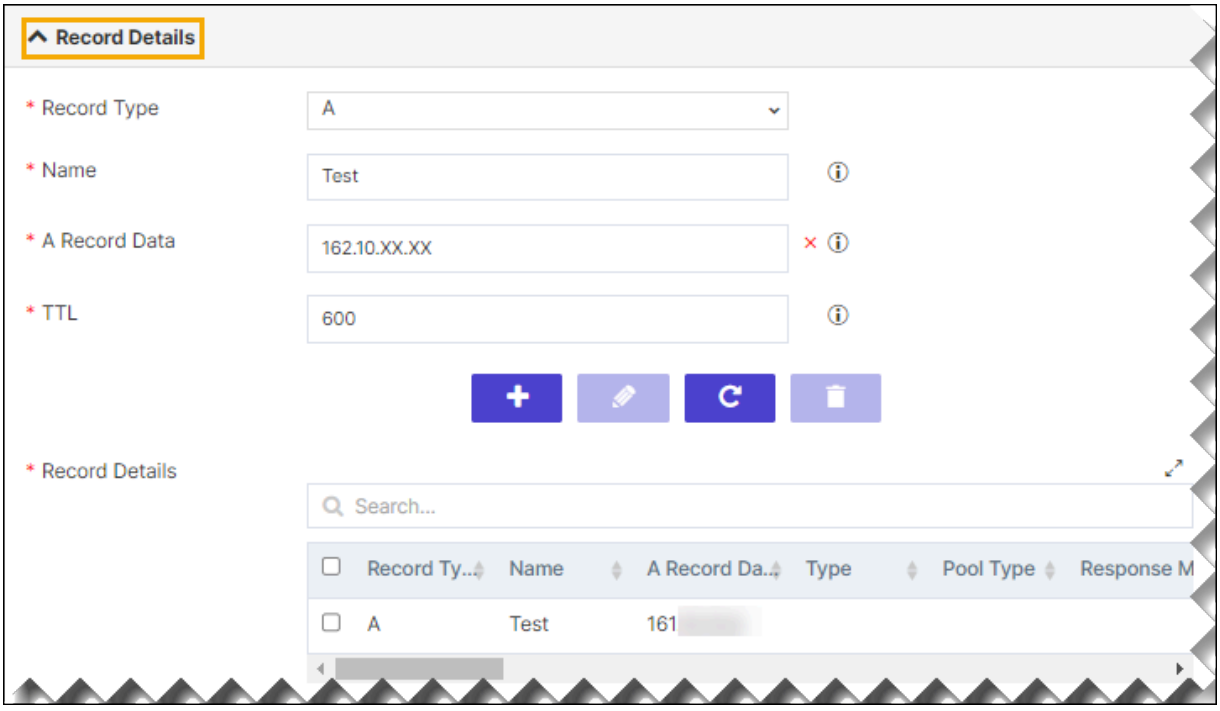
| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to create the record.<br>**Note:** The values in this field will be fetched based on the domain name search results. |
| ***DNS Provider** | Select the DNS provider from the options available in the dropdown. |

| Field | Description |
|---|---|
| | **Note:** The value(s) in this field will be fetched based on the domain name (TLD). For example, you can configure the TLD settings such that if the domain name selected is .net, the DNS Provider field will display Akamai or if the domain name selected is .org, then the DNS Provider field will display UltraDNS and so on. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.

**Note:** The fields displayed in this section will change depending on the **Record Type** selected.

7. To add the selected record details to the **Record Details** grid, click the (Add) icon.




8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the (**Pencil**) icon.

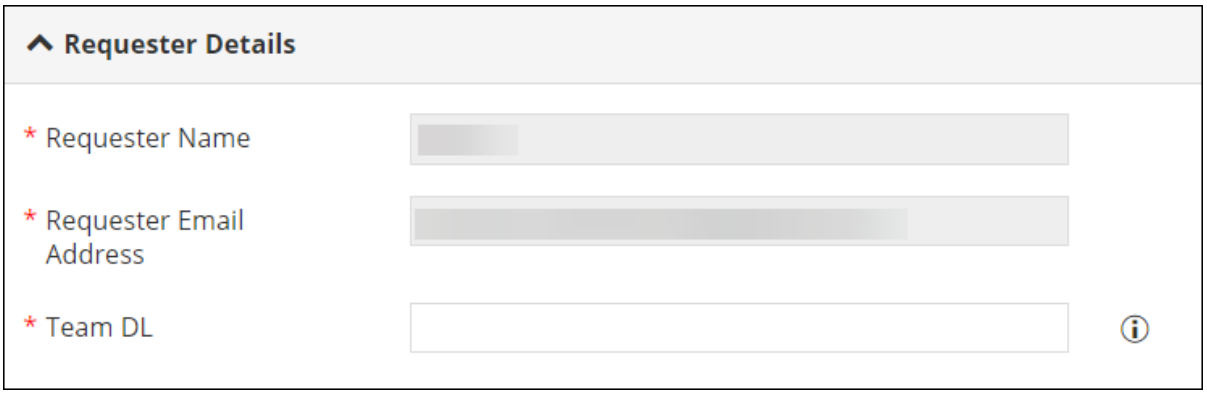
9. To delete a record detail, select the row to be deleted in the grid and click the (**Delete**) icon.
10. To maximize the **Record Details** grid, from the top right corner of the grid, click the (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.
13. At the **Zone Creation** stage of workflow execution, verify the information displayed and click **Submit**. DNS Record is created successfully.

## Decommissioning Domains

You can decommission domains that are no longer in use and delete them from the registrars.

To decommission a domain:

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Decommissioning Domains**. The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.




**Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **Domain Decommissioning** section, enter or select the required field information.

   The following table describes the field information in this section:

| Field | Description |
|---|---|
| ***Search Condition** | Select from the following search conditions:<br>• **Starts With**: Domains search result will list domains that start with the value provided in the next field.<br>• **Contains**: Domains search result will list domains that start with the value provided in the next field.<br>• **Ends With**: Domains search result will list domains that start with the value provided in the next field. |
| ***Search Domain Name** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Fetch Domains**.
   The values in the next field in the **Domain Decommissioning** section will be populated based on the information provided in the previous fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Select Domain** | Select the Domain from the options available in the dropdown.<br>**Note:** The values in this field will be fetched based on the domain name search results. |
| ***Vendor** | The vendor name is fetched automatically based on the domain name selection |
| ***Do you want to remove associated DNS Records?** | Select if you want to delete the DNS records associated with the selected domain name and vendor. |
| **: Mandatory fields* | |

6. Click **Submit**.
   An approval request is sent to the approver to approve or reject the domain decommissioning. Once the request is approved, the selected domain is decommissioned.

## Updating Domain Info

This workflow allows you to update the domain information in the AppViewX inventory.

To update the domain information:

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Update Domain Information**.
   The workflow execution page is displayed with the workflow inputs requested at the first stage.

   **Note:** In the **Requester Details** section, the field information will be fetched automatically from the logged in user information.

2. In the **Domain Info** section, enter or select the required field information.

   The following table describes the field information in this section:

| Field | Description |
|---|---|
| ***Search Condition** | Select from the following search conditions:<br>• **Starts With**: Domains search result will list domains that start with the search text provided in the next field.<br>• **Contains**: Domains search result will list domains that start with the search text provided in the next field.<br>• **Ends With**: Domains search result will list domains that start with the search text provided in the next field. |
| ***Search Domain Name** | Enter search text that is part of the domain name to show matching results. |
| **: Mandatory fields* | |

3. Click **Search Domains**.

   **Note:** The **Domain Name** field is auto-populated with domain names matching the search query.

4. Select the **Domain Name** for which the information has to be updated.
5. Select the **Domain Registrar** from the options available in the dropdown.

**Note:** The options available in the Domain Registrar field will vary according to the Domain Name selected.

6. Select if you want the **Auto Renewal** feature **On** or **Off**.
7. Enter the **NameServers** that will redirect traffic to the DNS servers.
8. Click **Submit**.

   The Domain information for the selected domain is updated.

## Generating Domain Expiry Report

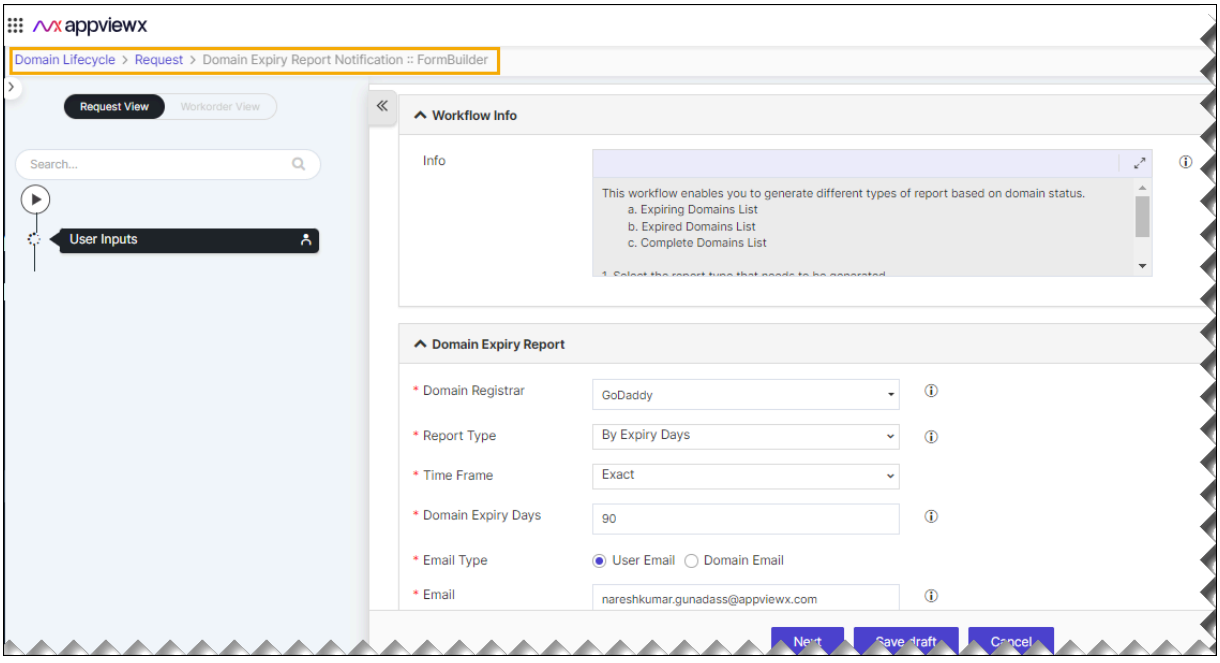
You can generate different reports displaying the domain statuses based on:

- Domains that have expired
- Domains that will expire in a specific number of days
- List of all domains

To generate any of these reports:

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Generate Domain Expiry Report**.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.



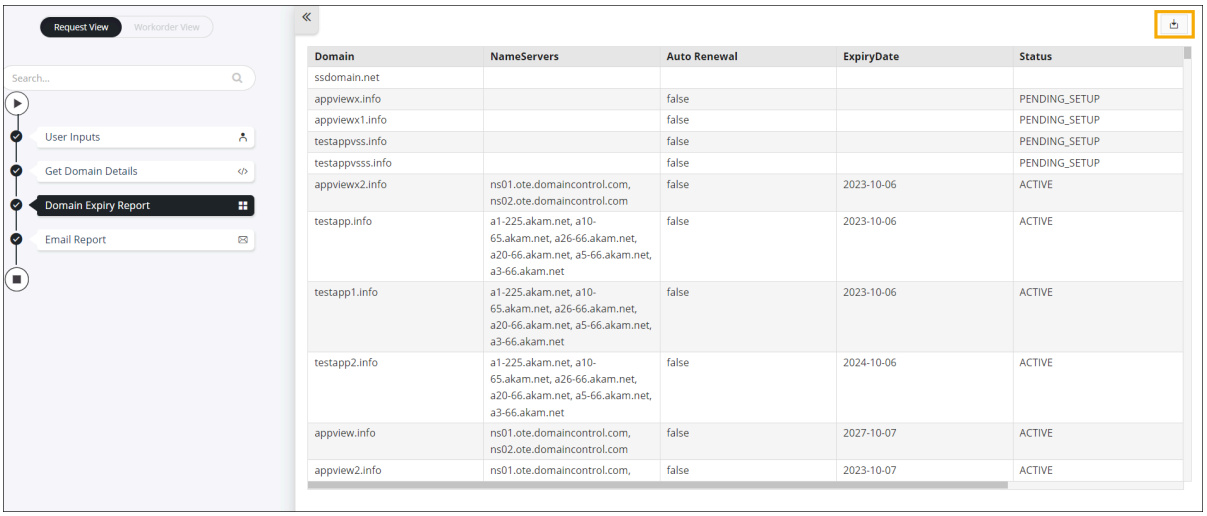

2. In the **Domain Expiry Report** section, enter or select the required field information.

The following table describes the fields in this section:

| Field | Description |
|---|---|
| ***Domain Registrar** | Select the configured domain registrar account from the options available in the dropdown. |
| ***Report Type** | Select the type of report you want to generate. The options available are:<br>• **By Expiry Days**: This generates a report listing the domains expiring within the specified number of days.<br>• **Expired Domains**: This generates a report listing all the expired domains.<br>• **Complete Report**: This generates a report listing all active and expired domains. |
| ***Domain Expiry Days** | Enter the number of days to the date of expiry, for which you want to generate a report. For example: If you enter the value 10, the report generated will display a list of domains expiring 10 days before the date of expiry.<br><br>**Note:** This field is displayed only when you select the option **By Expiry Days** in the **Report Type** field. |
| ***Email** | Enter the email address of the user to whom the report will be sent.<br><br>**Note:** You can enter multiple email addresses as comma-separated values. |
| **: Mandatory fields* | |

3. Click **Next**.

The **Domain Expiry Report** is generated. You can download it by clicking  from the top right corner of the screen.




## Creating Hosted Zones

A hosted zone contains records that store information on how the traffic for a specific domain should be routed.

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Create Hosted Zones**.
   The workflow execution page is displayed in a new tab with the workflow inputs requested at the first stage.

   **Note:** In the **User Details** section, the field information will be fetched automatically from the logged in user information.

2. In the **Zone Details** section, under **Domain Search**, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Search Condition** | Select from the following search conditions:<br>• **Starts With**: Domains search result will list domains that start with the search text provided in the next field.<br>• **Contains**: Domains search result will list domains that start with the search text provided in the next field.<br>• **Ends With**: Domains search result will list domains that start with the search text provided in the next field. |
| ***Search Domain Name** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

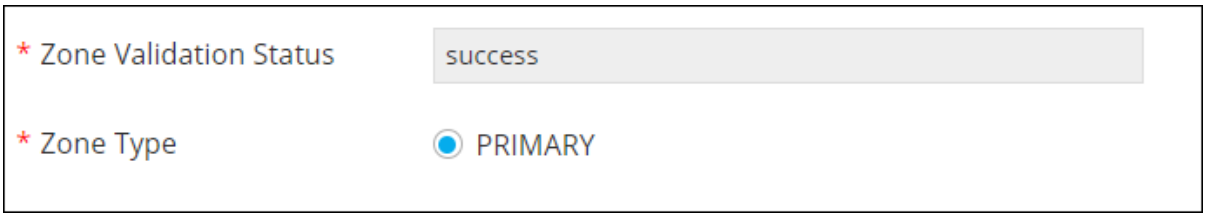
3. Click **Search Domains**.
   The values in the next fields in the **Zone Details** section will be populated based on the information provided in the above fields.
4. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Zone Name** | Select the Zone name from the options available in the dropdown.<br><br>**Note:** The values in this field are fetched based on the domain name search in the previous fields. |
| ***DNS Provider** | Select the DNS provider from the options available in the dropdown.<br><br>**Note:** The value(s) in this field will be fetched based on the domain name (TLD). For example, you can configure the TLD settings such that if the domain name selected is .net, the DNS Provider field will display Akamai or if the domain name selected is .org, then the DNS Provider field will display UltraDNS and so on. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |

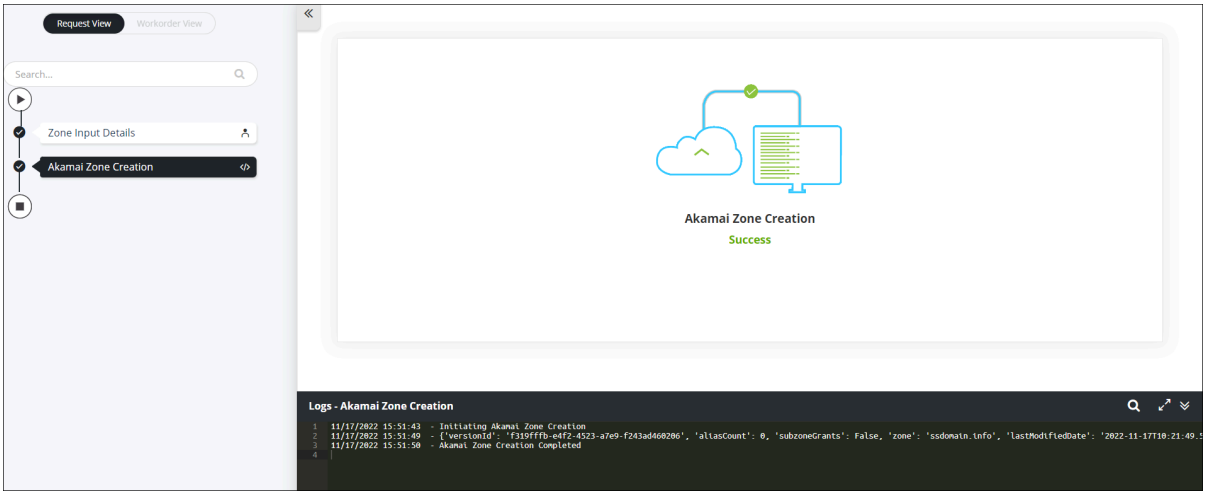
| Field | Description |
|---|---|
| | **Note:** The value(s) in this field are populated based on the option selected in the **DNS Provider** field. |
| **: Mandatory fields* | |

5. To check if a zone is available, click **Zone Availability**.
   A zone availability check runs in the background and the **Zone Validation Status** is updated as success or failure.




**Note:** Currently only primary **Zone Type** is supported.

6. Click **Submit**.
   The hosted zone is created successfully.

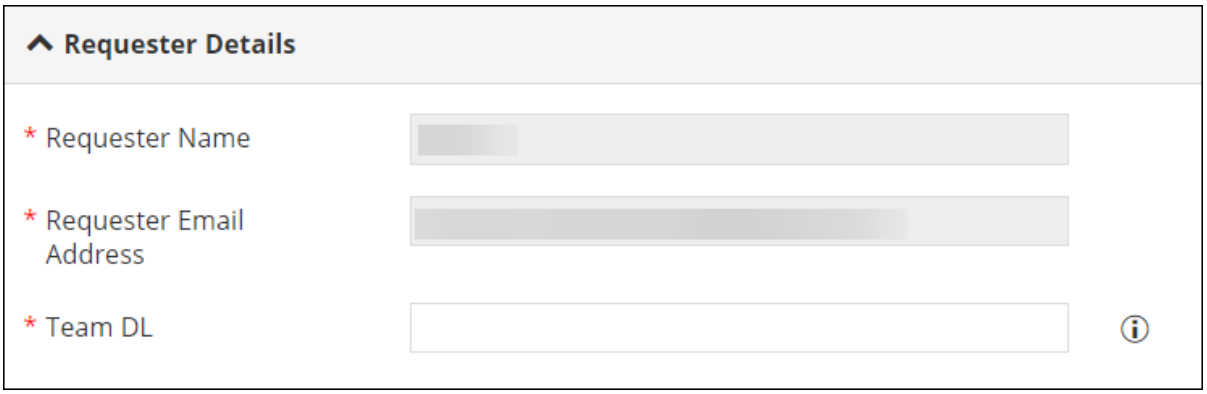



## Renewing a Domain

A domain is typically registered for a period of one year. At the end of the year, the domain can be decommissioned (if not in use) or renewed. AppViewX facilitates the automation of the domain renewal process.

To renew a domain:

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Renew Domains**.
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.




> **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **Domain Search** section, enter or select the required field information.

   The following table describes the field information in this section:

| Field | Description |
|---|---|
| ***Search By** | Select if you want to search the domain that you want to renew by:<br>• **Domain Name**: You can use this option when you know the specific domain that needs to be renewed.<br>• **Expiry Days**: You can use this option when you want to renew domain(s) expiring within a specific number of days |
| ***Domain Name** | Enter the domain name that you want to renew.<br>**Note:** This field is displayed only when you select **Domain Name** in the **Search By** field. |
| ***Domain Expiry Days** | Enter the number of days till the expiry of the domain. |

| Field | Description |
|---|---|
| | **Note:** This field is displayed only when you select **Expiry Days** in the **Search By** field. |
| **Get Domains** | Click this button to get a list of domains that are expiring within the number of days specified in the **Domain Expiry Days** field. |
| ***Expiry Domains List** | Select the domain(s) that you want to renew from the dropdown list.<br>**Note:** This list is populated only when you click the Get Domains button. |
| **: Mandatory fields* | |

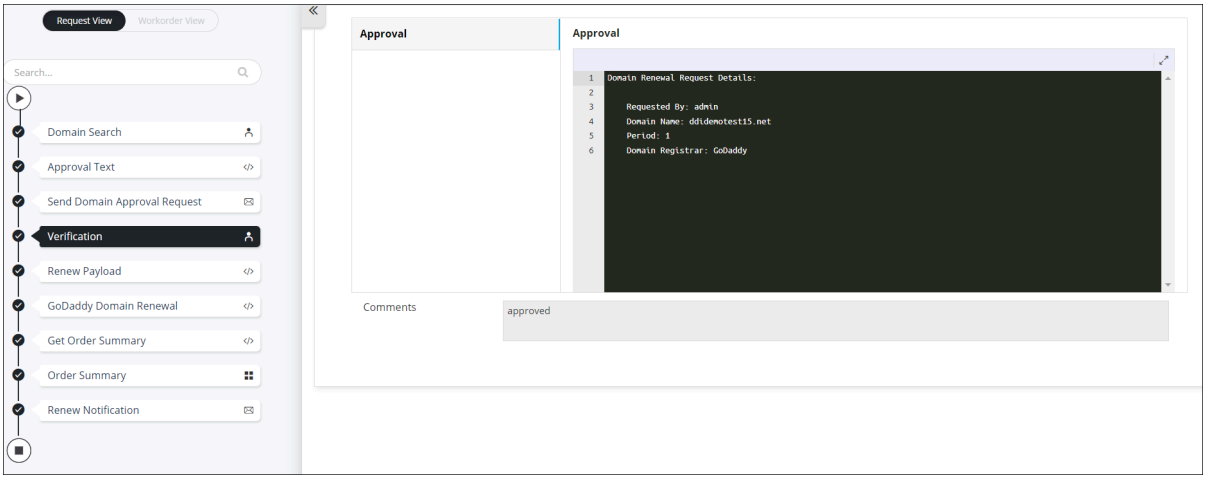
4. In the **Domain Information** section, enter the required field information.

   The following table describes the field information in this section:

| Field | Description |
|---|---|
| ***Domain Name** | Displays the name of the domain that is to be renewed based on the selection in the **Domain Search** section.<br>**Note:** This is an auto-populated, read-only field. |
| ***Domain ID** | Displays the domain ID of the domain to be renewed.<br>**Note:** This is an auto-populated, read-only field. |
| ***Expiring At** | Displays the date on which the domain will expire.<br>**Note:** This is an auto-populated, read-only field. |
| ***Validity Period (Years)** | Enter the number of years for which this domain is to be renewed. |
| **Name Servers** | Enter the name server details. |
| **: Mandatory fields* | |

5. Click **Submit**.

Domain renewal is approved and Domain Renewal notification is sent to the requester.



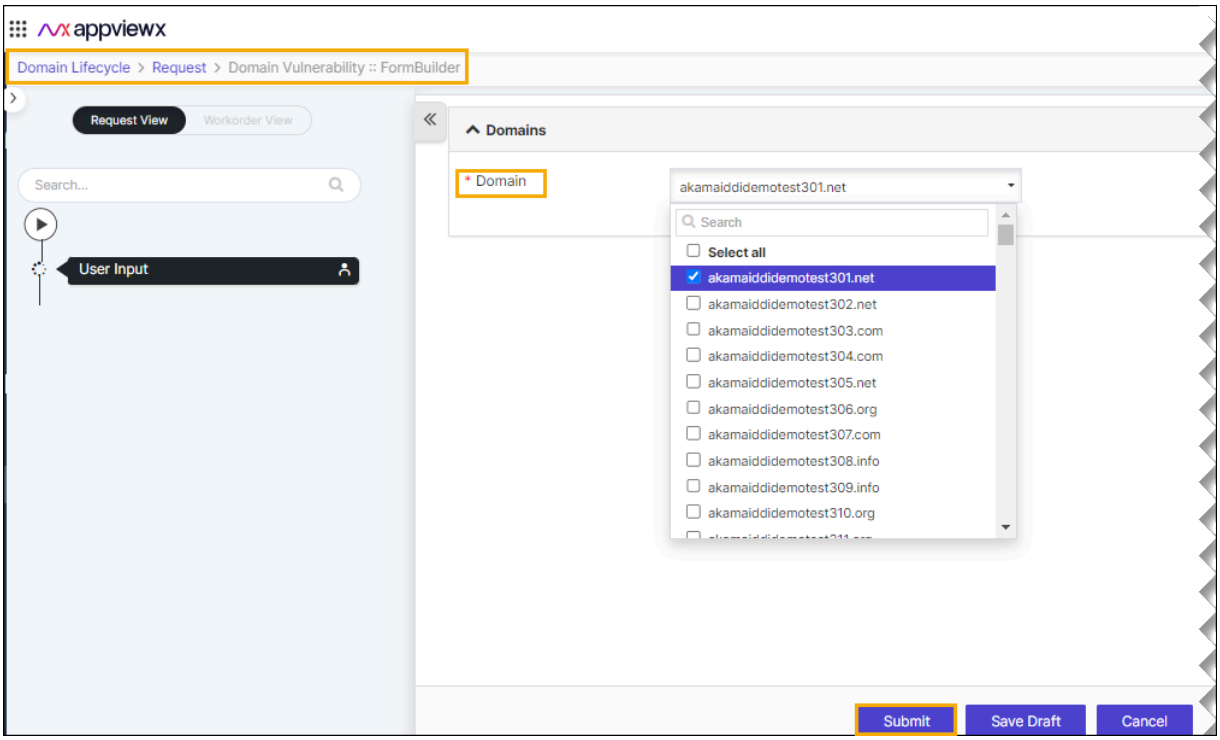

6. For more details on the renewal order, go to the **Order Summary** stage of the workflow.

## Domain Vulnerability

A domain vulnerability enables the scanning of potential vulnerabilities across domains and sub-domains. It categorizes these vulnerabilities based on various scan types including HTTPS/HTTP Scan, CNAME Scan, MX Record Scan, SPF Record Scan, DMARC Scan, and NS Scan.

To create a domain vulnerability:

1. Go to **DDI+** > **Self Service** > **Domain Lifecycle**, and then click **Domain Vulnerability**.
   The workflow execution page is displayed with the workflow inputs requested at the first stage.




2. In the **Domains** section, in the **Domain** field, select the desired domain vulnerability that you want submit.
3. Click **Submit**.

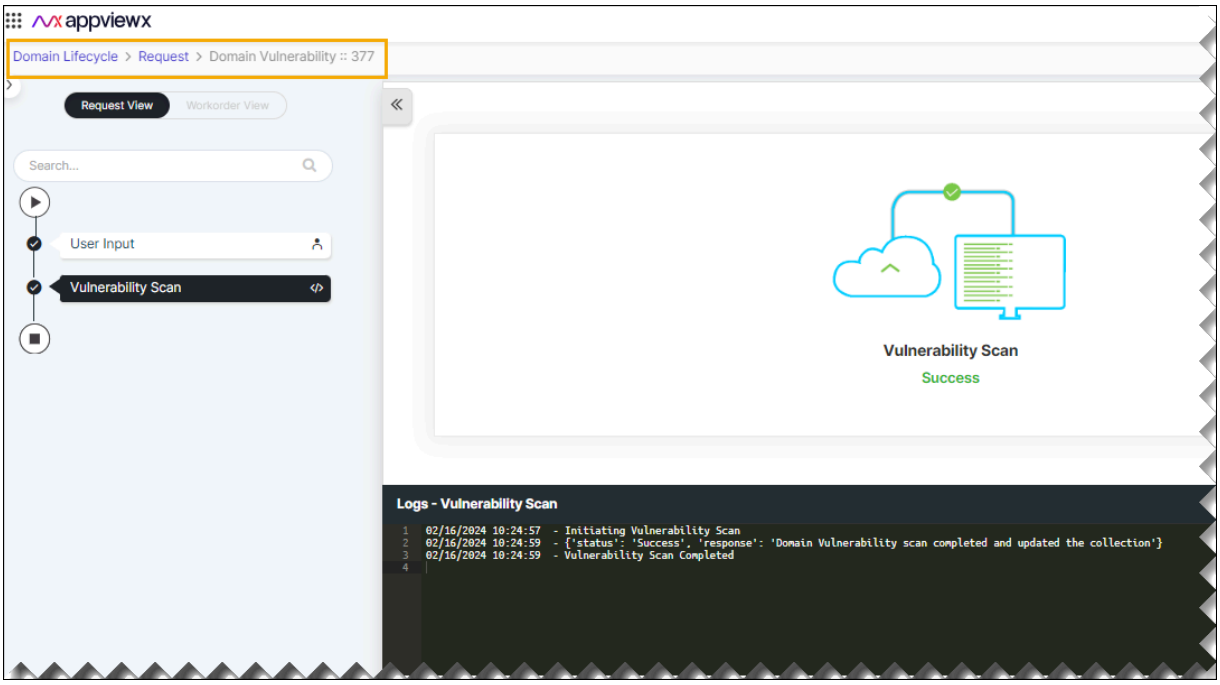
   The pop-up message appears as

   > Are you sure you want to Submit?

4. Click **Ok**.

   The pop-up message appears as

   > Request ID 123 Submitted Successfully.




5. For more details on the domain vulnerability, go to the **Domain Vulnerability Insights** dashboard.

## DNS Automation

The DNS Automation section displays all workflows specific to DNS and domain lifecycle management, categorized under catalogs. The following workflow catalogs are available here:

- AWS Route53
- Ultra DNS
- Akamai Edge DNS
- Infoblox IPAM
- Bluecat IPAM
- Alerts and Notifications.

- AWS Route53 Automation Catalog
- Ultra DNS Automation Catalog
- Akamai Edge Grid Automation Catalog
- Microsoft Automation Catalog

- Infoblox IPAM Automation Catalog
- Bluecat IPAM Automation Catalog

## AWS Route53 Automation Catalog

The following workflows are available under this catalog:

- Creating Route53 DNS Records
- Creating Route53 Hosted Zone
- Modifying Route53 DNS Records
- Deleting Route53 DNS Records

## Creating Route53 DNS Records

DNS records provide information about domains such as IP address(es) associated with that domain, handling requests for the domain, and so on.

To create a Route53 DNS record:

1. In the **DNS Automation** section, under the **AWS Route53** catalog, hover your mouse over the **Create Route53 DNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** You can go back to the **DNS Automation** page by clicking  (**Back arrow**) from the top left corner of the page.

2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Route53). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to create the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click the  (**Add**) icon.
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the  (**Pencil**) icon.
9. To delete a record detail, select the row to be deleted in the grid and click the  (**Delete**) icon.
10. To maximize the **Record Details** grid, from the top right corner of the grid, click the  (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Creating Route53 Hosted Zone

A hosted zone contains records that store information on how the traffic for a specific domain should be routed.

To create a Route53 hosted zone:

1. In the **DNS Automation** section, under the **Akamai Edge DNS** catalog, hover your mouse over the **Create Akamai Edge Hosted Zone** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** In the **User Details** section, the field information will be fetched automatically from the logged in user information. You can go back to the **DNS Automation** page by clicking from the top left corner of the page.

2. In the **Zone Details** section, enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the name of the DNS Provider (in this case, Akamai). |
| ***DNS Provider Account** | Select the DNS provider account in which the Hosted Zone will be created from the options available in the dropdown.<br>**Note:** The value(s) in this field are populated based on the option selected in the **DNS Provider** field. |
| ***Domain Name** | Enter a valid domain name to create the hosted zone. For example: app.com, prod.app.com |
| **: Mandatory fields* | |

3. To check if a zone is available, click **Zone Validation**.

   **Note:** Currently only Primary **Zone Type** is supported.

A zone availability check runs in the background and the **Zone Validation Status** is updated as success or failure.

4. Click **Submit**.

## Modifying Route53 DNS Records

This workflow allows you to modify the record type, name, and other record details.

To modify a Route53 DNS record:

1. In the **DNS Automation** section, under the **AWS Route53** catalog, hover your mouse over the **Modify Route53 DNS Records** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** You can go back to the **DNS Automation** page by clicking the (**Back arrow**) icon from the top left corner of the page.

2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Route53). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.

The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.

5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to modify the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click  .
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click  .
9. To delete a record detail, select the row to be deleted in the grid and click  .
10. To maximize the **Record Details** grid, from the top right corner of the grid, click  .
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Deleting Route53 DNS Records

You can delete a DNS record(s) and completely remove them from your zone file when it is no longer needed or the TTL (Time To Live) for the record expires.

To delete a Route53 DNS record:

1. In the **DNS Automation** section, under the **AWS Route53** catalog, hover your mouse over the **Delete Route53 DNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** You can go back to the **DNS Automation** page by clicking  from the top left corner of the page.

2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Route53). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to delete the record. |

| Field | Description |
|---|---|
| | **Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click  .
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click  .
9. To delete a record detail, select the row to be deleted in the grid and click  .
10. To maximize the **Record Details** grid, from the top right corner of the grid, click  .
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Ultra DNS Automation Catalog

The following workflows are available under this catalog:

- Creating UltraDNS Records
- Creating UltraDNS Hosted Zone
- Modifying UltraDNS Records
- Deleting UltraDNS Records

## Creating UltraDNS Records

DNS records provide information about domains such as IP address(es) associated with that domain, handling requests for the domain, and so on.

To create a UltraDNS record:

1. In the **DNS Automation** section, under the **UltraDNS** catalog, hover your mouse over the **Create UltraDNS Records** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** You can go back to the **DNS Automation** page by clicking (**Back arrow**) icon from the top left corner of the page.

2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (UltraDNS). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to create the record. |

| Field | Description |
|---|---|
| | **Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click .
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click .
9. To delete a record detail, select the row to be deleted in the grid and click .
10. To maximize the **Record Details** grid, from the top right corner of the grid, click .
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Creating UltraDNS Hosted Zone

A hosted zone contains records that store information on how the traffic for a specific domain should be routed.

To create a UltraDNS hosted zone:

1. In the **DNS Automation** section, under the **UltraDNS** catalog, hover your mouse over the **Create UltraDNS Hosted Zone** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** In the **User Details** section, the field information will be fetched automatically from the logged in user information.

2. In the **Zone Details** section, enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the name of the DNS Provider (in this case, Akamai). |
| ***DNS Provider Account** | Select the DNS provider account in which the Hosted Zone will be created from the options available in the dropdown.<br><br>**Note:** The value(s) in this field are populated based on the option selected in the **DNS Provider** field. |
| ***Domain Name** | Enter a valid domain name to create the hosted zone. For example: app.com, prod.app.com |
| **: Mandatory fields* | |

3. To check if a zone is available, click **Zone Validation**.

   **Note:** Currently only Primary **Zone Type** is supported.

   A zone availability check runs in the background and the **Zone Validation Status** is updated as success or failure.
4. Click **Submit**.

## Modifying UltraDNS Records

This workflow allows you to modify the record type, name, and other record details.

To modify a UltraDNS record:

1. In the **DNS Automation** section, under the **UltraDNS** catalog, hover your mouse over the **Modify UltraDNS Records** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

> **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (UltraDNS). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to modify the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **All * marked fields are mandatory.** | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click  .
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click  .
9. To delete a record detail, select the row to be deleted in the grid and click  .

10. To maximize the **Record Details** grid, from the top right corner of the grid, click  .
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Deleting UltraDNS Records

You can delete a DNS record(s) and completely remove them from your zone file when it is no longer needed or the TTL (Time To Live) for the record expires.

To delete a UltraDNS record:

1. In the **DNS Automation** section, under the **UltraDNS** catalog, hover your mouse over the **Delete UltraDNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (UltraDNS). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to delete the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click the (**Add**) icon.
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the (**Pencil**) icon.
9. To delete a record detail, select the row to be deleted in the grid and click the (**Delete**) icon.
10. To maximize the **Record Details** grid, from the top right corner of the grid, click the (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Akamai Edge Grid Automation Catalog

The following workflows are available under this catalog:

- Creating Akamai Edge DNS Records
- Creating Akamai Edge Hosted Zone
- Modifying Akamai Edge DNS Records
- Deleting Akamai Edge DNS Records

## Creating Akamai Edge DNS Records

DNS records provide information about domains such as IP address(es) associated with that domain, handling requests for the domain, and so on.

To create a Akamai Edge DNS record:

1. In the **DNS Automation** section, under the **Akamai Edge DNS** catalog, hover your mouse over the **Create Akamai Edge DNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Akamai). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to create the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |

| Field | Description |
|---|---|
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click the  (**Add**) icon.
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the  (**Pencil**) icon.
9. To delete a record detail, select the row to be deleted in the grid and click the  (**Delete**) icon.
10. To maximize the **Record Details** grid, from the top right corner of the grid, click the  (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Creating Akamai Edge Hosted Zone

A hosted zone contains records that store information on how the traffic for a specific domain should be routed.

To create a Akamai Edge hosted zone:

1. In the **DNS Automation** section, under the **Akamai Edge DNS** catalog, hover your mouse over the **Create Akamai Edge Hosted Zone** workflow, and then click the  (**Play**) icon.
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   > **Note:** In the **User Details** section, the field information will be fetched automatically from the logged in user information.

2. In the **Zone Details** section, enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the name of the DNS Provider (in this case, Akamai). |
| ***DNS Provider Account** | Select the DNS provider account in which the Hosted Zone will be created from the options available in the dropdown.<br><br>**Note:** The value(s) in this field are populated based on the option selected in the **DNS Provider** field. |
| ***Domain Name** | Enter a valid domain name to create the hosted zone. For example: app.com, prod.app.com |
| **: Mandatory fields* | |

3. To check if a zone is available, click **Zone Validation**.

   **Note:** Currently only Primary **Zone Type** is supported.

   A zone availability check runs in the background and the **Zone Validation Status** is updated as success or failure.
4. Click **Submit**.

## Modifying Akamai Edge DNS Records

This workflow allows you to modify the record type, name, and other record details.

To modify a Akamai Edge DNS record:

1. In the **DNS Automation** section, under the **Akamai Edge DNS** catalog, hover your mouse over the **Modify Akamai Edge DNS Records** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

**Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Akamai). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to modify the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click the (**Add**) icon.
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the (**Pencil**) icon.
9. To delete a record detail, select the row to be deleted in the grid and click the (**Delete**) icon.

10. To maximize the **Record Details** grid, from the top right corner of the grid, click the  (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Deleting Akamai Edge DNS Records

You can delete a DNS record(s) and completely remove them from your zone file when it is no longer needed or the TTL (Time To Live) for the record expires.

To delete a Akamai Edge DNS record:

1. In the **DNS Automation** section, under the **Akamai Edge DNS** catalog, hover your mouse over the **Delete Akamai Edge DNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Akamai). |
| ***Search Domain** | Enter the search text/keywords for searching the domains. |
| **: Mandatory fields* | |

4. Click **Search Domains**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Domain Name** | Select the **Domain Name** from the options available in the dropdown list, to delete the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click the (**Add**) icon.
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the (**Pencil**) icon.
9. To delete a record detail, select the row to be deleted in the grid and click the (**Delete**) icon.
10. To maximize the **Record Details** grid, from the top right corner of the grid, click the (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Microsoft Automation Catalog

The following workflows are available under this catalog:

- Creating Microsoft DNS Records
- Creating Microsoft DNS Zone
- Modifying Microsoft DNS Records
- Deleting Microsoft DNS Records

## Creating Microsoft DNS Records

DNS records provide information about domains such as IP address(es) associated with that domain, handling requests for the domain.

To create a Microsoft DNS record:

1. In the **DNS Automation** section, under the **Microsoft DNS** catalog, hover your mouse over the **Create Microsoft DNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** You can go back to the **DNS Automation** page by clicking  (**Back arrow**) icon from the top left corner of the page.

2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (Microsoft). |
| ***Search Zone** | Enter the search text/keywords for searching the zones. |
| **: Mandatory fields* | |

4. Click **Search Zones**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Zone Name** | Select the **Zone Name** from the options available in the dropdown list, to create the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click .
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click .
9. To delete a record detail, select the row to be deleted in the grid and click .
10. To maximize the **Record Details** grid, from the top right corner of the grid, click .
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Creating Microsoft DNS Zone

A hosted zone contains records that store information on how the traffic for a specific domain should be routed.

To create a Microsoft DNS zone:

1. In the **DNS Automation** section, under the **Microsoft DNS** catalog, hover your mouse over the **Create Microsoft DNS Zone** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** In the **User Details** section, the field information will be fetched automatically from the logged in user information.

2. In the **Zone Details** section, enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the name of the DNS Provider (in this case, Microsoft). |
| ***DNS Provider Account** | Select the DNS provider account in which the Zone will be created from the options available in the dropdown.<br><br>**Note:** The value(s) in this field are populated based on the option selected in the **DNS Provider** field. |
| ***Server** | Select the server from the dropdown list. |
| ***Zone Name** | Enter a valid zone name to create the zone. For example: app.com, prod.app.com |
| **: Mandatory fields* | |

3. To check if a zone is available, click **Zone Validation**.

   **Note:** Currently only Primary **Zone Type** is supported.

   A zone availability check runs in the background and the **Zone Validation Status** is updated as success or failure.
4. Click **Submit**.

## Modifying Microsoft DNS Records

This workflow allows you to modify the record type, name, and other record details.

To modify a Microsoft DNS record:

1. In the **DNS Automation** section, under the **Microsoft DNS** catalog, hover your mouse over the **Modify Microsoft DNS Records** workflow and click .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (UltraDNS). |
| ***Search Zone** | Enter the search text/keywords for searching the Zones. |
| **: Mandatory fields* | |

4. Click **Search Zones**.
   The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.
5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Zone Name** | Select the **Zone Name** from the options available in the dropdown list, to modify the record.<br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **All * marked fields are mandatory.** | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click +.

8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click  .
9. To delete a record detail, select the row to be deleted in the grid and click  .
10. To maximize the **Record Details** grid, from the top right corner of the grid, click  .
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Deleting Microsoft DNS Records

You can delete a DNS record(s) and completely remove them from your zone file when it is no longer needed or the TTL (Time To Live) for the record expires.

To delete a Microsoft DNS record:

1. In the **DNS Automation** section, under the **Microsoft DNS** catalog, hover your mouse over the **Delete Microsoft DNS Records** workflow and click  .
   The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.
2. In the **Requester Details** section, in the **Team DL** field, enter the email addresses to which the domain registration email should be sent. Multiple email addresses must be entered as comma-separated values.

   **Note:** The field information for the first two fields will be fetched automatically from the logged in user information.

3. In the **DNS Details** section, enter or select the required field information.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***DNS Provider** | This is a read only field and displays the DNS Provider name (UltraDNS). |
| ***Search Zone** | Enter the search text/keywords for searching the zones. |
| **: Mandatory fields* | |

4. Click **Search Zones**.

The values in the next fields in the **DNS Details** section will be populated based on the information provided in the above fields.

5. Enter or select the required field information in the remaining fields.

   The following table describes the field information required here:

| Field | Description |
|---|---|
| ***Zone Name** | Select the **Zone Name** from the options available in the dropdown list, to delete the record.<br><br>**Note:** The values in this field will be fetched based on the search keywords entered in the previous fields. |
| ***DNS Provider Account** | Select the DNS provider account from the options available in the dropdown. |
| **: Mandatory fields* | |

6. In the **Record Details** section, enter or select the required field information.
7. To add the selected record details to the **Record Details** grid, click the  (**Add**) icon.
8. To edit the record details in the **Record Details** grid, select the row, modify the details, and click the  (**Pencil**) icon.
9. To delete a record detail, select the row to be deleted in the grid and click the  (**Delete**) icon.
10. To maximize the **Record Details** grid, from the top right corner of the grid, click the  (**Expand**) icon.
11. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
12. Click **Submit**.

## Infoblox IPAM Automation Catalog

The following workflows are available under this catalog:

Workflows under this catalog are categorized under three headings:

- Create
  - Create Infoblox DNS records - Basic
  - Create Infoblox DNS Zone

- Modify
  - Modify Infoblox DNS records - Basic
  - Modify Infoblox DNS records - Advanced
  - Modify Infoblox DNS Zone
- Delete
  - Delete Infoblox DNS records - Basic
  - Delete Infoblox DNS records - Advanced
  - Delete Infoblox DNS Zone
- Creating Infoblox DNS Zone

## Creating Infoblox DNS Zone

A hosted zone contains records that store information on how the traffic for a specific domain should be routed. This workflow enables the user to create a DNS zone in Infoblox.

To create a Infoblox DNS zone:

1. In the **DNS Automation** section, under the **Infoblox IPAM** catalog, click **Create Infoblox DNS Zone**. The workflow execution page is displayed in the same tab with the workflow inputs requested at the first stage.

   **Note:** In the **Requester Details** section, the field information will be fetched automatically from the logged in user information.

2. In the **Zone Details** section, enter or select the required field information.

   The following table describes the required field information:

| Field | Description |
|---|---|
| ***Device Name** | Select the device where the DNS zone will be created. |
| ***Zone Type** | Select the zone type from the drop-down list.<br>• Authoritative<br>• Forward<br>• Delegate. |
| **Network View** | Select the network view from the drop-down. |

| Field | Description |
|---|---|
| ***DNS View** | Select the DNS view for the zone from the drop-down. |
| ***Zone** | Enter the DNS zones that represent your DNS zone of authority. For example, appviewx.com. |
| **Comment** | Enter the required comment. |
| **: Mandatory fields* | |

3. In the **Zone Validations** section, click **Zone Availability** to check if a zone is available.
   A zone availability check runs in the background and the **Zone Validation Status** is updated as success or failure.
4. Click **Submit**.

## Bluecat IPAM Automation Catalog

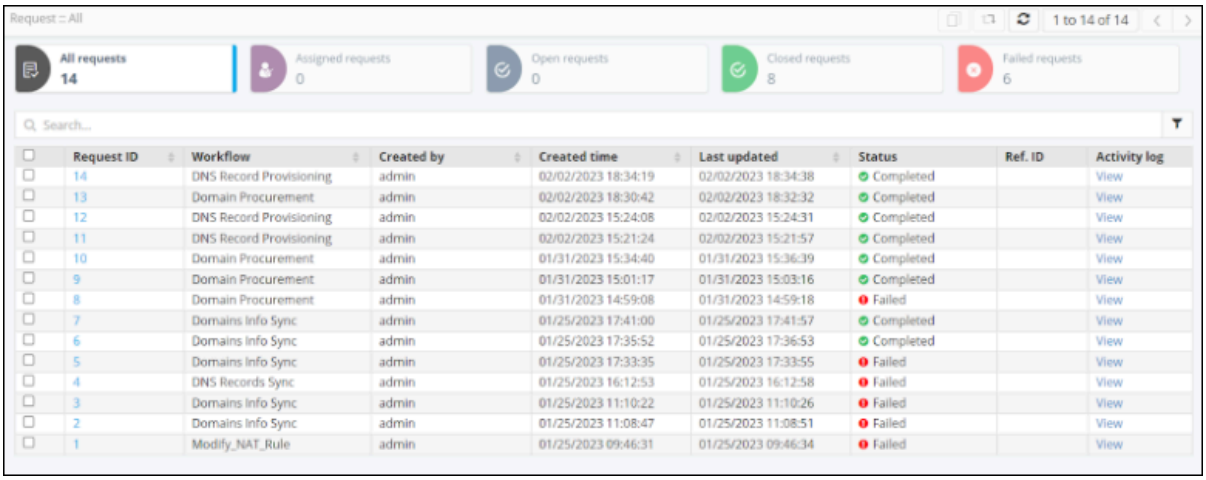
Workflows under this catalog are categorized under three headings:

- Create
  - Create Bluecat DNS records
- Modify
  - Modify Infoblox DNS records
- Delete
  - Delete Infoblox DNS records

**Note:** For more information on these workflows refer to the ADC Automation Workflow User Guide.

## Viewing Service Requests

All the workflow requests triggered from the DDI+ module can be viewed in one place in the **Service Requests** section.




This page displays the following information:

| | |
|---|---|
| **All requests** | The total number of requests triggered for domain and DNS management. |
| **Assigned requests** | The total number of requests assigned to a particular user. |
| **Open requests** | The total number of open requests (requests that are still running) in DDI+ module. |
| **Closed requests** | The total number of closed requests (requests successfully triggered and completed) in DDI+ module. |
| **Failed requests** | The total number of failed requests (requests that did not execute successfully) in DDI+ module. |

1. To see the stage-wise execution of a workflow, click on the **Request ID** for that workflow.
2. To clone a service request, select the request and click the (**Clone**) icon from the command bar in the top right corner of the screen.
3. To refresh the page, from the command bar in the top right corner of the page, click the (**Refresh**) icon.
4. To view the stage-wise summary and work order logs for each service request, under the **Activity log** column, click **View**.

# Chapter 2: DDI+ Admin Guide

This guide describes the process of setting up and getting started with DDI+. It also provides information on integrating the domain registrars and DNS providers.



## Setting up the Proxy

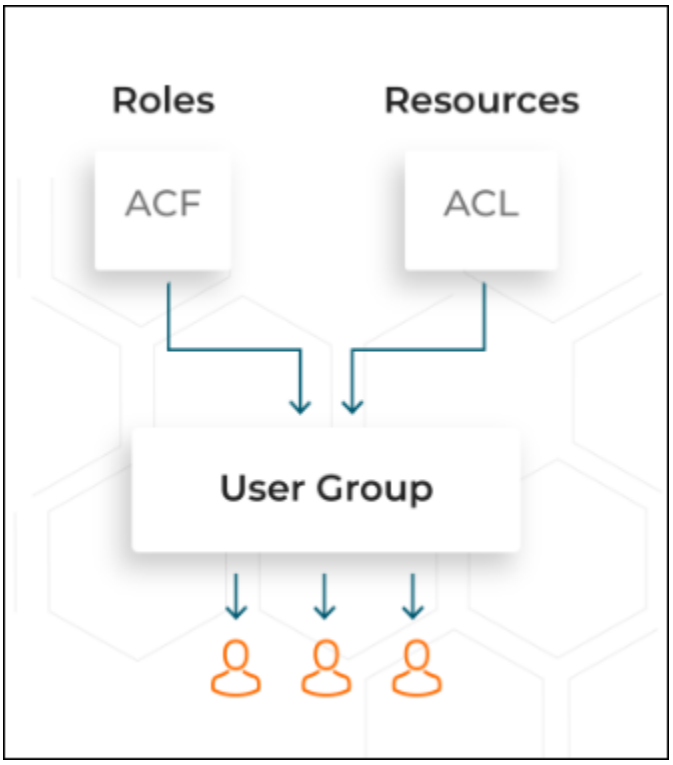
For steps on how to set up the proxy, refer to the Platform User Guide.

## Configuring the SMTP Settings

For steps on how to configure the SMTP settings, refer to the Platform User Guide.

## Configuring Role Based Access Control

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC). RBAC is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise. It allows you to integrate with the existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and resources can be customized to suit any organizational structure and user requirements.

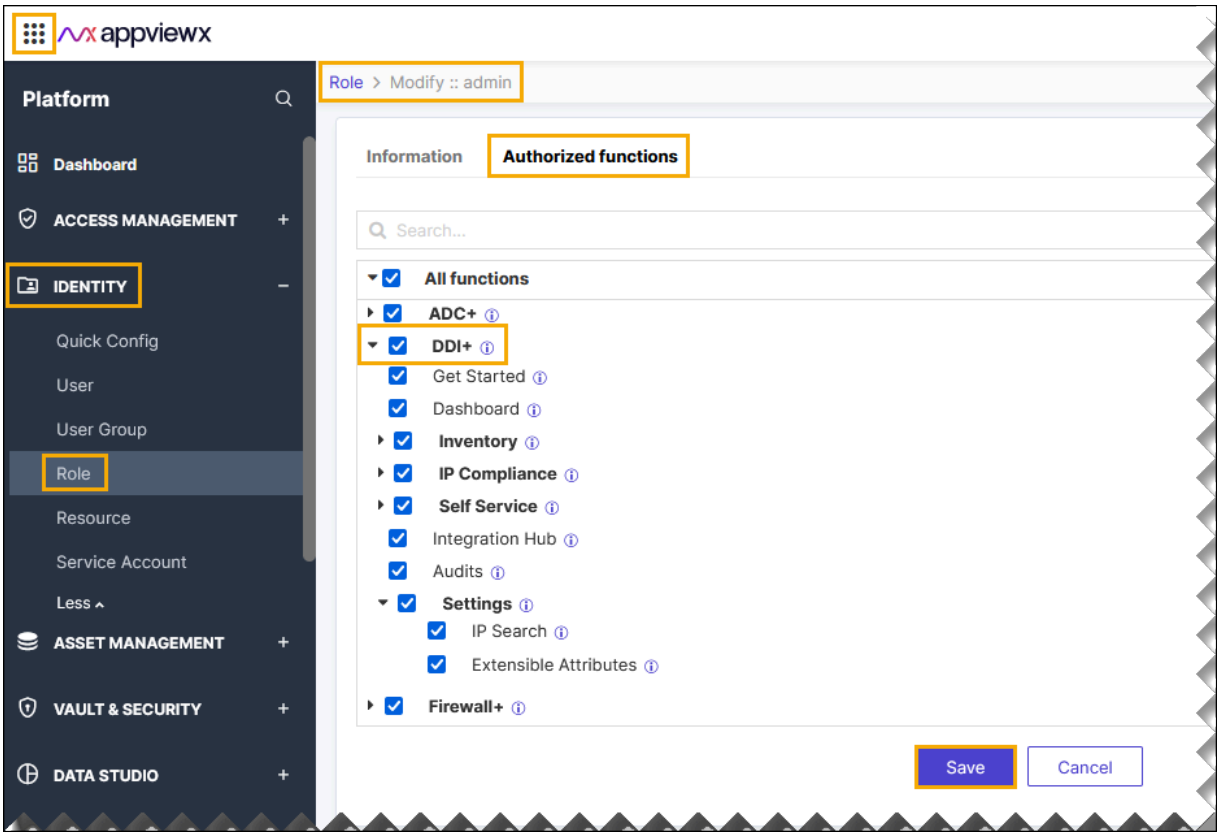



RBAC lets employees have access rights only to the AppViewX functions and network resources they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

To get an overview of the actions authorized for a particular user in the DDI+ module:

| New Menu | Old Menu |
|---|---|
| In the **Platform** module, from the left pane, under **IDENTITY**, select **Role**.<br>The **Role** page is displayed, with all the roles listed with their **Name**, **Description**, and **Status**. | From the main menu, select **Account** > **Role**.<br>The **Role** page is displayed, with all the roles listed with their **Name**, **Description**, and **Status**. |
| **Note:** For more information on how to switch between menus, click here. | |

1. On the **Role** page, select a role from the dropdown list, for example **admin**.
2. To see the list of permissions that can be defined for this role, under the **Authorized Functions** tab, click ▶ to expand **DDI**. A selected check-box indicates that the corresponding action has been authorized in the DDI+ module.

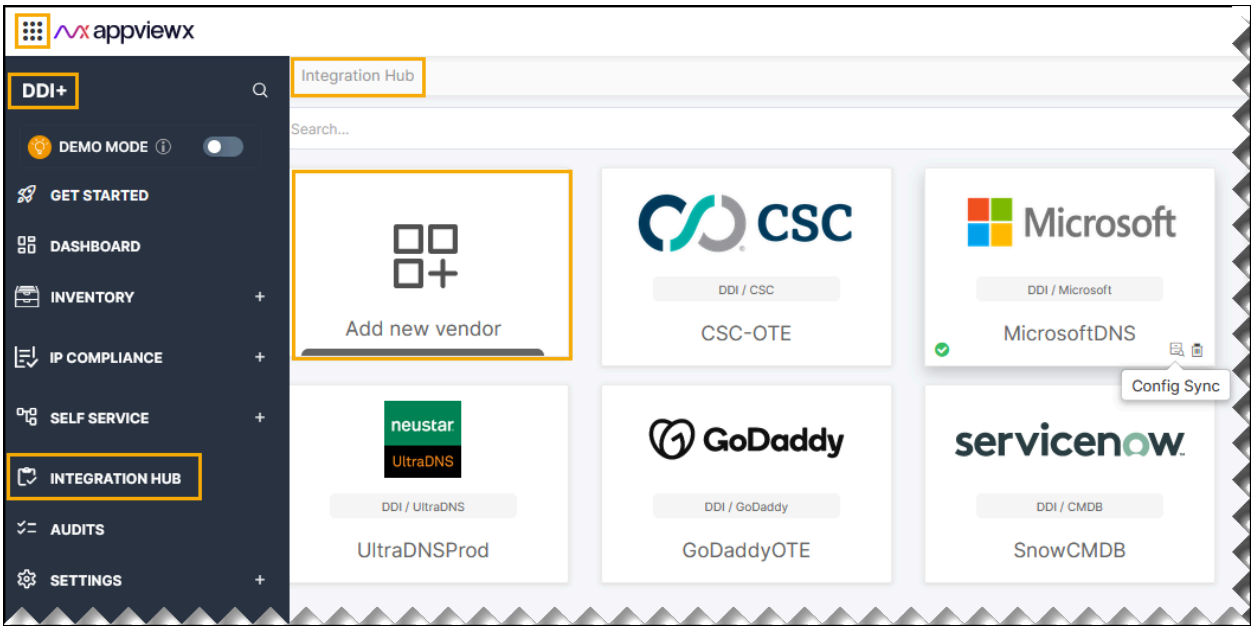



The following table describes the various actions that can be authorized or restricted in the **DDI+** module:

| Action | Description |
|---|---|
| **Get Started** | Access to get started page of the DDI+ module. |
| **Dashboard** | Access to all the dashboards that are associated with the DDI+ module. |
| **Inventory** | Access to all the inventories that are associated with the DDI+ module. |
| **IP Compliance** | Access to IP compliance of DDI+ module. |
| **Self Service** | Access to Self Service of DDI+ module. |
| **Integration Hub** | Access to Integration Hub of DDI+ module. |
| **Audits** | Access to Audits of DDI+ module. |
| **Settings** | Access to Settings of DDI+ module. |

# Integration Hub

The DDI+ Integration Hub allows users to seamlessly integrate enterprise domain registrars, DNS providers, IP Address Management (IPAM), and Configuration Management Database (CMDB) systems with the DDI+ platform. This streamlines the management of DNS infrastructure, providing centralized control through a unified interface.




- Onboarding Domain Registrars
- Onboarding DNS providers and IPAM
- Onboarding CMDB
- Configuring Other Vendor
- Integration Hub Vendor Actions

## Onboarding Domain Registrars

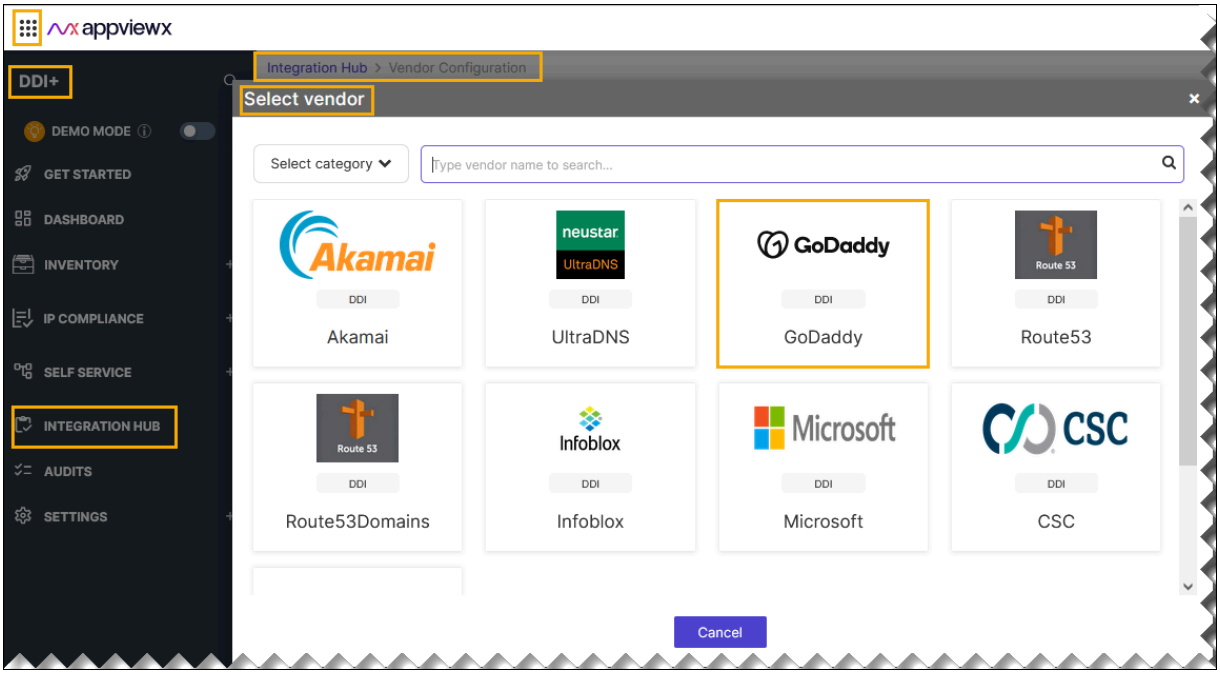
Integrate one or multiple domain registrar accounts into DDI+ Integration Hub across various vendors.

- Configuring GoDaddy
- Configuring CSC
- Configuring Route53Domains
- Configuring Clouflare DNS

## Configuring GoDaddy

To configure GoDaddy:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **GoDaddy**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **API Key** method of authentication selected by default. |
| ***Key** | Enter the authorization key. |
| ***Add to** | Select **Header** from the dropdown list if not already selected. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Value** | Enter the authorization value. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes.


**Sample Schema**:

```
{
    "businessUnits": [
        "Sales",
        "Marketing",
        "Finance"
    ],
    "consent": {
```

```
    "aggrementKeys": [
        "DNRA"
    ],
    "aggredBy": "sample host/ip"
},
"domain_price_limit": 10,
"approver_email": "test@example.com",
"nameServerConfig": [
    {
        "supported_domains": [
            ".com",
            ".org",
            ".in",
            ".biz"
        ],
        "auto_fetch": false,
        "vendor": "",
        "vendor_account_name": "",
        "nameservers": [
            "test1.ns.com",
            "test2.ns.com"
        ]
    },
    {
        "supported_domains": [
            ".net",
            ".info"
        ],
        "auto_fetch": false,
        "vendor": "SampleVendor",
        "vendor_account_name": "SampleVendorAccount",
        "nameservers": []
    }
],
"contacts": {
    "contactAdmin": {
        "addressMailing": {
```

```
            "address1": "Sample Address",
            "address2": "Sample Address",
            "city": "Sample City",
            "country": "Sample Country",
            "postalCode": "Sample Code",
            "state": "Sample State"
        },
        "email": "test@example.com",
        "fax": "",
        "nameFirst": "Sample Name",
        "nameLast": "Sample Name",
        "organization": "Sample Organization",
        "phone": "12346768990"
    },
    "contactBilling": {
        "addressMailing": {
            "address1": "Sample Address",
            "address2": "Sample Address",
            "city": "Sample City",
            "country": "Sample Country",
            "postalCode": "Sample Code",
            "state": "Sample State"
        },
        "email": "test@example.com",
        "fax": "",
        "nameFirst": "Sample Name",
        "nameLast": "Sample Name",
        "organization": "Sample Organization",
        "phone": "12346768990"
    },
    "contactRegistrant": {
        "addressMailing": {
            "address1": "Sample Address",
            "address2": "Sample Address",
            "city": "Sample City",
            "country": "Sample Country",
            "postalCode": "Sample Code",
```

```
            "state": "Sample State"
        },
        "email": "test@example.com",
        "fax": "",
        "nameFirst": "Sample Name",
        "nameLast": "Sample Name",
        "organization": "Sample Organization",
        "phone": "12346768990"
    },
    "contactTech": {
        "addressMailing": {
            "address1": "Sample Address",
            "address2": "Sample Address",
            "city": "Sample City",
            "country": "Sample Country",
            "postalCode": "Sample Code",
            "state": "Sample State"
        },
        "email": "test@example.com",
        "fax": "",
        "nameFirst": "Sample Name",
        "nameLast": "Sample Name",
        "organization": "Sample Organization",
        "phone": "12346768990"
    }
  },
  "requestorMapping": {
    "requestor_email": "test@example.com"
  }
}
```


The following table explains the strings in the JSON schema:

| Strings | Description |
|---|---|
| aggredBy | Originating client IP address of the end-user's computer when they consented to these legal agreements. |

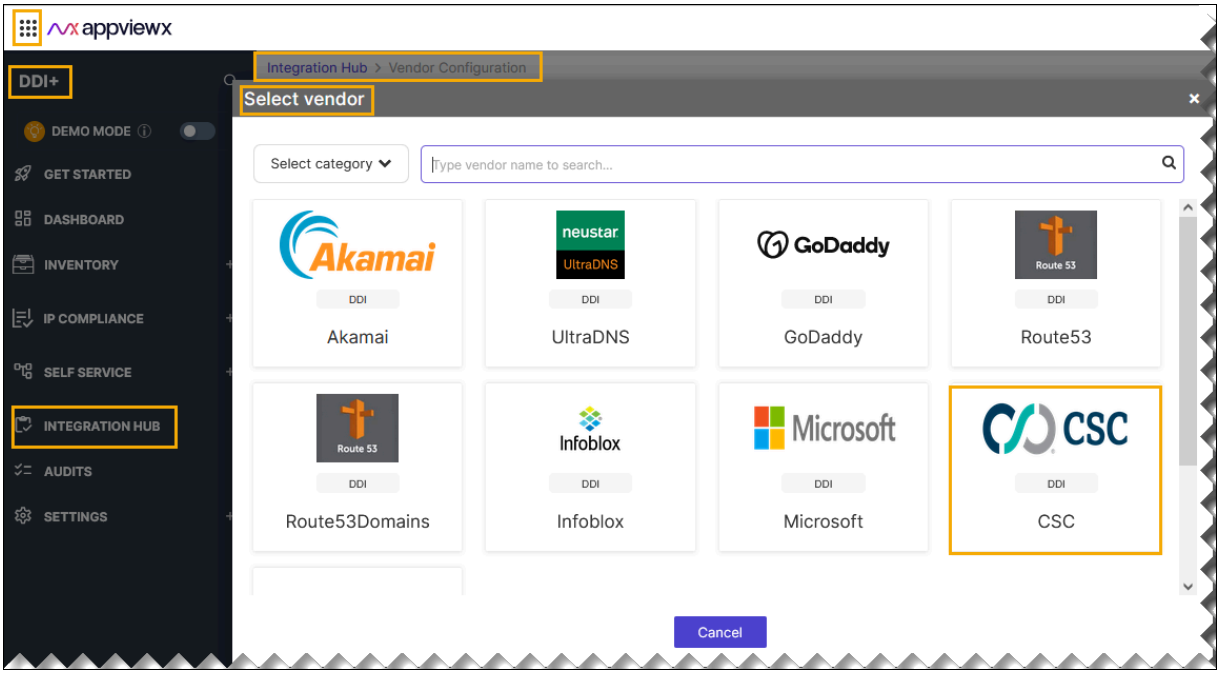
| Strings | Description |
|---|---|
| aggrementKeys | Unique identifiers of the legal agreements to which the end-user has agreed, as returned from the/domains/agreements endpoint as DNRA. |
| domain_price_limit | The domain_price_limit field serves to establish a threshold price for domain registrations. If the cost of a domain surpasses the value set in domain_price_limit, explicit approval is mandated for the registration. If the domain's price falls below the domain_price_limit, no approval is necessary. |
| approver_email | The approver_email field is to trigger an email notification for approval when the price of a domain registration exceeds the specified domain_price_limit. If the cost surpasses this limit, an email is automatically sent to the designated approver for review and confirmation |
| nameServerConfig | The nameServerConfig field is configured to facilitate the automatic selection of nameservers based on predefined conditions during the domain registration process |
| supported_domains | explicitly define the list of Top-Level Domains (TLDs) permitted for use in the domain procurement process, particularly when configured nameservers are in use. Like [".com", ".net" ] |
| auto_fetch | used to automatically retrieve the name server information from the configured name server account in AppViewX |
| vendor | The vendor field is to specify the DNS vendor from which the name server should be automatically fetched. This is applicable only if the auto fetch is true. |
| vendor_account_name | The vendor_account_name field is used to specify vendor account name configured in AppViewX, specifically for automatically fetching the nameserver. This configuration is applicable only when the auto_fetch flag is set to true |
| nameservers | The 'nameservers' string is utilized to indicate the list of all nameservers to be assigned during domain registration. This is relevant only when the 'auto_fetch' flag is set to false, as in: ["example1.ns.com", "example2.ns.com"]. |
| **: Mandatory fields* | |

7. Click **Finish**.

## Configuring CSC

To configure CSC:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **CSC**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **API Key** method of authentication selected by default. |
| ***Key** | Enter the authorization key. |
| ***Add to** | Select **Header** from the dropdown list if not already selected. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Value** | Enter the authorization value. |
| ***Custom Header** | Click the custom header radio button. |
| **Custom Header Config** | Enter the valid API key and its corresponding value. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes.


**Sample Schema**:

```
{
"domain_price_limit": 10,
"businessUnits": [
"Sales",
"Marketing",
```

```
"Finance"
],
"CSCbusinessUnit": "Sample business Unit",
"accountNumber": 123455,
"nameServerConfig": [
{
"supported_domains": [
".com",
".org",
".in",
".biz"
],
"auto_fetch": false,
"vendor": "",
"vendor_account_name": "",
"nameservers": [
"test1.ns.com",
"test2.ns.com"
]
},
{
"supported_domains": [
".net",
".info"
],
"auto_fetch": false,
"vendor": "SampleVendor",
"vendor_account_name": "SampleVendorAccount",
"nameservers": []
}
],
"whoisContacts": {
"registrantProfile": "CSC Registrant",
"adminProfile": "CSC Admin",
"technicalProfile": "CSC Tech"
},
"notes": "sample text",
```

```
"notifications": {
"enabled": false,
"additionalNotificationEmails": [
"test1@example.com",
"test2@example.com"
]
},
"brand": "Sample text",
"redactPublicWhois": true,
"showPrice": true,
"customFields": [
{
"name": "Business Owner",
"value": ""
},
{
"name": "Comments",
"value": ""
}
],
"approver_email": "test@example.com"
}
```


The following table explains the strings in the JSON schema:

| Strings | Description |
|---|---|
| CSCbusinessUnit | The business unit's code configured in CSC domain manager. |
| accountNumber | Account number provided by CSC Global. |
| registrantProfile | Profile name of registrar contact. |
| adminProfile | Profile name of admin contact. |
| technicalProfile | Profile name of Technical Contact. |
| notes | Provide decription for domain if needed |
| notifications > enabled | Send notifications to recipents if enabled. |
| additionalNotificationEmails | Provide recipients mail address if notification enabled. |

| Strings | Description |
|---|---|
| brand | Provide brand name if needed. |
| redactPublicWhois | If you want to conceal contact information from WHOIS queries. If you specify true, WHOIS ("who is") queries return contact information for CSC Global Registrar. |
| customFields | Name and value of the custom fields as defined in Domain Manager. |
| domain_price_limit | The domain_price_limit field serves to establish a threshold price for domain registrations. If the cost of a domain surpasses the value set in domain_price_limit, explicit approval is mandated for the registration. If the domain's price falls below the domain_price_limit, no approval is necessary. |
| approver_email | The approver_email field is to trigger an email notification for approval when the price of a domain registration exceeds the specified domain_price_limit. If the cost surpasses this limit, an email is automatically sent to the designated approver for review and confirmation. |
| nameServerConfig | The nameServerConfig field is configured to facilitate the automatic selection of nameservers based on predefined conditions during the domain registration process. |
| auto_fetch | Used to automatically retrieve the name server information from the configured name server account in AppViewX. |
| vendor | The vendor field is to specify the DNS vendor from which the name server should be automatically fetched. This is applicable only if the auto fetch is true. |
| vendor_account_name | The vendor_account_name field is used to specify vendor account name configured in AppViewX, specifically for automatically fetching the nameserver. This configuration is applicable only when the auto_fetch flag is set to true. |
| nameservers | The nameservers is used to specify the list of all the nameservers to be assigned during the domain registration. This is applicable only when the auto_fetch flag is set to false. like ["example1.ns.com", "example2.ns.com"]. |

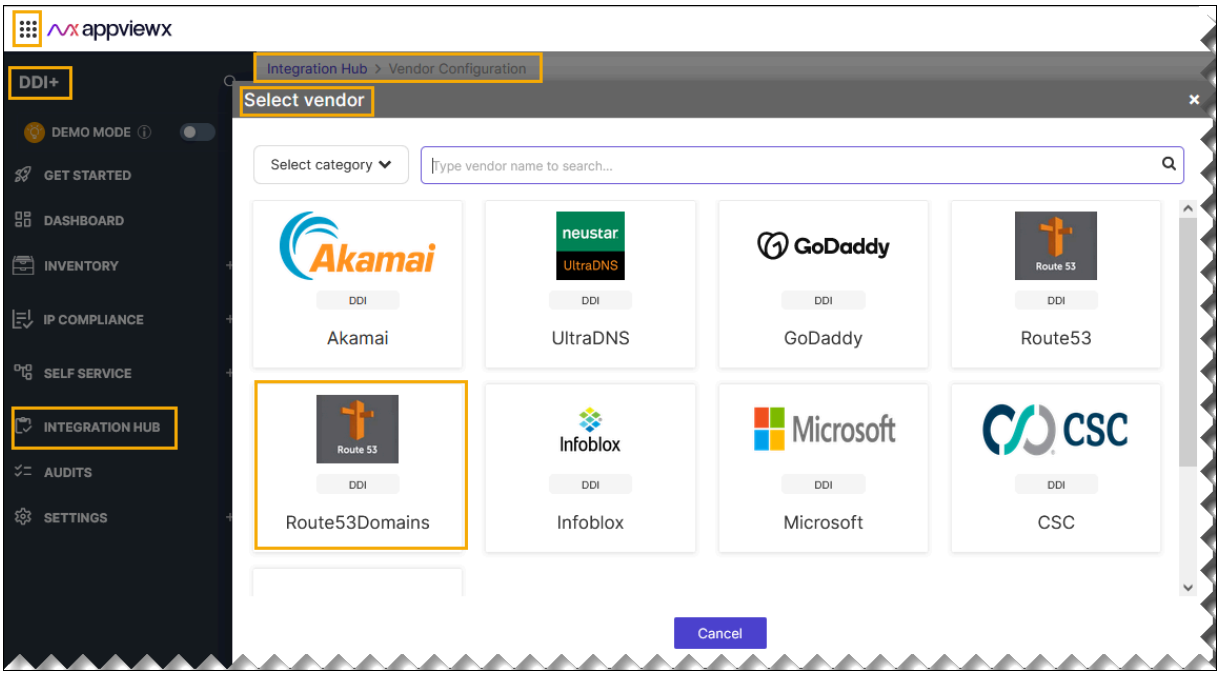
| Strings | Description |
|---|---|
| *: Mandatory fields | |

7. Click **Finish**.

## Configuring Route53Domains

To configure Route53Domains:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Route53Domains**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |

| Field | Description |
|---|---|
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **AWS signature** method of authentication selected by default. |
| ***Access Key** | Enter the Access Key provided by route53domains. |
| ***AWS Region** | Enter the region which is receiving the request. |
| **Session Token** | Enter the session token which is only required when using temporary security credentials. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol |
| ***Secret Key** | Enter the Secret Key provided by route53domains. |
| ***Service Name** | This field is filled by default. The service which is receiving a request. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Config** toggle to add additional vendor configuration attributes.


**Sample Schema**:


```
{
  "businessUnits": [
    "Sales",
    "Marketing",
    "Finance"
  ],
  "domain_price_limit": 10,
  "approver_email": "test@example.com",
  "nameServerConfig": [
    {
      "supported_domains": [
        ".com",
        ".org",
        ".in",
        ".biz"
      ],
      "auto_fetch": false,
      "vendor": "",
      "vendor_account_name": "",
      "nameservers": [
        "test1.ns.com",
        "test2.ns.com"
```

```
        ]
    },
    {
        "supported_domains": [
            ".net",
            ".info"
        ],
        "auto_fetch": false,
        "vendor": "SampleVendor",
        "vendor_account_name": "SampleVendorAccount",
        "nameservers": []
    }
],
"contacts": {
    "AdminContact": {
        "FirstName": "Sample Name",
        "MiddleName": "Sample Name",
        "LastName": "Sample Name",
        "ContactType": "Sample Type",
        "OrganizationName": "Sample Organization",
        "AddressLine1": "Sample Address",
        "AddressLine2": "Sample Address",
        "City": "Sample City",
        "State": "Sample State",
        "CountryCode": "Sample Code",
        "ZipCode": "Sample Code",
        "PhoneNumber": "Sample Phone",
        "Email": "Sample Email",
        "Fax": "Sample Fax"
    },
    "RegistrantContact": {
        "FirstName": "Sample Name",
        "MiddleName": "Sample Name",
        "LastName": "Sample Name",
        "ContactType": "Sample Type",
        "OrganizationName": "Sample Organization",
        "AddressLine1": "Sample Address",
```

```
        "AddressLine2": "Sample Address",
        "City": "Sample City",
        "State": "Sample State",
        "CountryCode": "Sample Code",
        "ZipCode": "Sample Code",
        "PhoneNumber": "Sample Phone",
        "Email": "Sample Email",
        "Fax": "Sample Fax"
      },
      "TechContact": {
        "FirstName": "Sample Name",
        "MiddleName": "Sample Name",
        "LastName": "Sample Name",
        "ContactType": "Sample Type",
        "OrganizationName": "Sample Organization",
        "AddressLine1": "Sample Address",
        "AddressLine2": "Sample Address",
        "City": "Sample City",
        "State": "Sample State",
        "CountryCode": "Sample Code",
        "ZipCode": "Sample Code",
        "PhoneNumber": "Sample Phone",
        "Email": "Sample Email",
        "Fax": "Sample Fax"
      }
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```


The following table explains the strings in the JSON schema:

| Strings | Description |
|---|---|
| PrivacyProtectAdminContact | Whether you want to conceal contact information from WHOIS queries. If you specify true, WHOIS ("who is") queries return |

| Strings | Description |
|---|---|
| | contact information for the registrar, the phrase "REDACTED FOR PRIVACY", or "On behalf of domain name's owner." |
| PrivacyProtectRegistrantContact | Whether you want to conceal contact information from WHOIS queries. If you specify true, WHOIS ("who is") queries return contact information either for Amazon Registrar (for .com, .net, and .org domains) or for our registrar associate, Gandi (for all other TLDs). If you specify false, WHOIS queries return the information that you entered for the registrant contact (domain owner). |
| PrivacyProtectTechContact | Whether you want to conceal contact information from WHOIS queries. If you specify true, WHOIS ("who is") queries return contact information either for Amazon Registrar (for .com, .net, and .org domains) or for our registrar associate, Gandi (for all other TLDs). If you specify false, WHOIS queries return the information that you entered for the technical contact. |
| AdminContact | Provides detailed contact information. |
| RegistrantContact | Provides detailed contact information. |
| TechContact | Provides detailed contact information. |
| domain_price_limit | The domain_price_limit field serves to establish a threshold price for domain registrations. If the cost of a domain surpasses the value set in domain_price_limit, explicit approval is mandated for the registration. If the domain's price falls below the domain_price_limit, no approval is necessary. |
| approver_email | The approver_email field is to trigger an email notification for approval when the price of a domain registration exceeds the specified domain_price_limit. If the cost surpasses this limit, an email is automatically sent to the designated approver for review and confirmation |
| nameServerConfig | The nameServerConfig field is configured to facilitate the automatic selection of nameservers based on predefined conditions during the domain registration process |

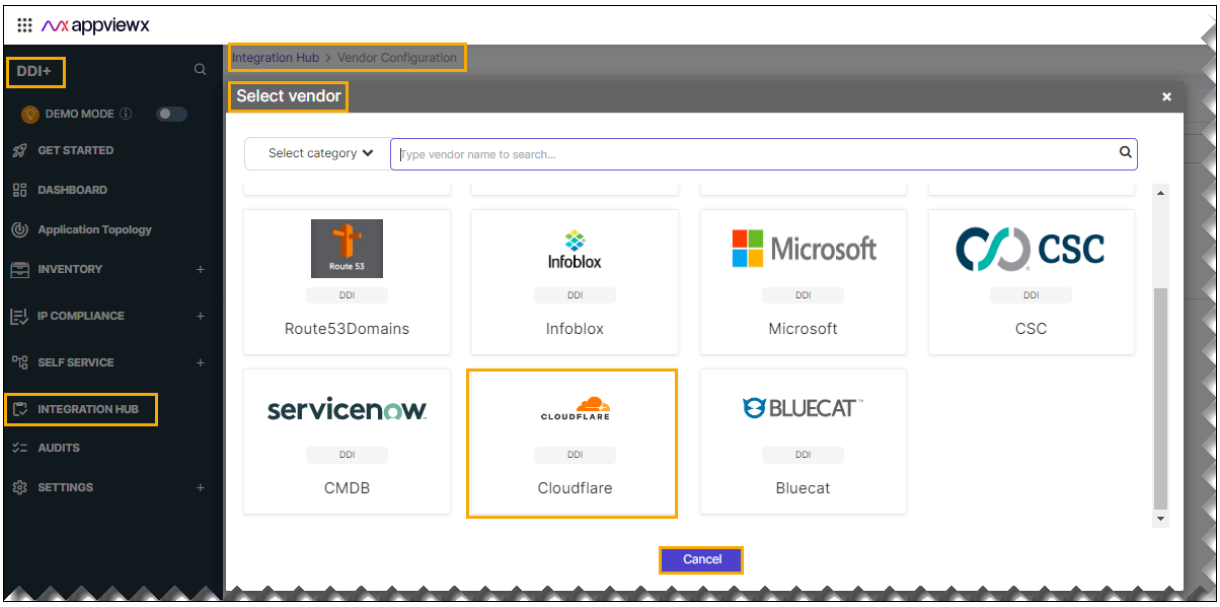
| Strings | Description |
|---|---|
| supported_domains | Explicitly define the list of Top-Level Domains (TLDs) permitted for use in the domain procurement process, particularly when configured nameservers are in use. Like [".com", ".net" ] |
| auto_fetch | The auto_fetch used to automatically retrieve the name server information from the configured name server account in AppViewX. |
| vendor | The vendor field is to specify the DNS vendor from which the name server should be automatically fetched. This is applicable only if the auto fetch is true. |
| vendor_account_name | The vendor_account_name field is used to specify vendor account name configured in AppViewX, specifically for automatically fetching the nameserver. This configuration is applicable only when the auto_fetch flag is set to true |
| nameservers | The nameservers is used to specify the list of all the nameservers to be assigned during the domain registration. This is applicable only when the auto_fetch flag is set to false. like ["example1.ns.com", "example2.ns.com"]. |
| **: Mandatory fields* | |

7. Click **Finish**.

## Configuring Clouflare DNS

To configure Cloudflare DNS:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Cloudflare**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **Bearer Token** method of authentication selected by default. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***** **Token** | Enter the authentication URL to obtain an access token to authenticate Cloudflare APIs. |

| Field | Description |
|---|---|
| ***Account ID** | Enter the Cloudflare account ID for API integration |
| **: Mandatory fields* | |

5. Enable **Use Proxy** for the vendor.
6. Enable **Config sync** for parsing the vendor.
7. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes.
8. Click **Finish**.

## Onboarding DNS providers and IPAM

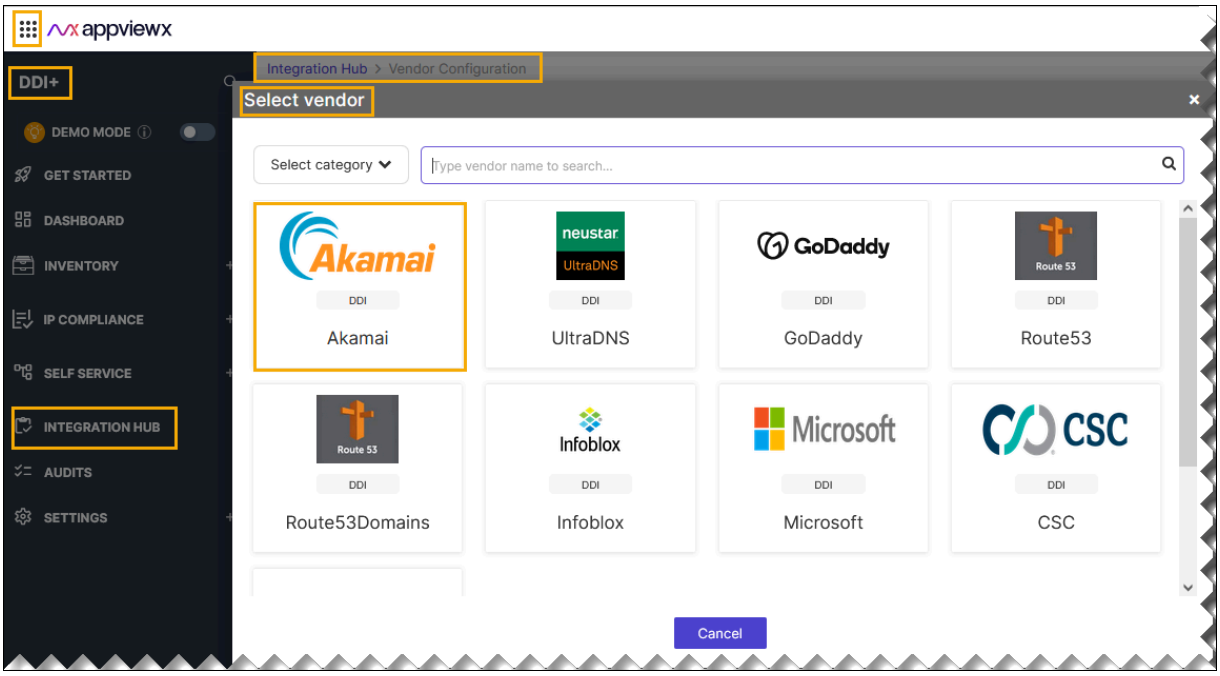
Integrate Managed and Private DNS vendors, as well as IPAM systems, into the DDI+ Integration Hub.

- Configuring Akamai
- Configuring UltraDNS
- Configuring Route53
- Configuring Microsoft
- Configuring Infoblox
- Configuring Bluecat
- Configuring Micetro

## Configuring Akamai

To configure Akamai:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Akamai**.
3. On the **Vendor Configuration** page, under the **General** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **Akamai EdgeGrid** method of authentication selected by default. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |

| Field | Description |
|---|---|
| ***Access Token** | Enter the Access token provided by Akamai. |
| ***Client Secret** | Enter the Client secret provided by Akamai. |
| ***Client Token** | Enter the Client token provided by Akamai. |
| ***Contract ID** | Enter the Akamai contract id for API integration. |
| **Advanced Configs** | If you want to enter the more details click the advanced configs radio button.<br>**Note:** Default values are automatically generated for some of these below fields unless values are |

| Fields | Description |
|---|---|
| ***Nonce** | Random string generated by the client. |
| ***Timestamp** | UTC time in such format as specified in the API client authentication section of the Aka portal. |
| ***Base URL** | Enter the base URL, without the protocol. |
| ***Headers to sign** | Comma-separated list of headers needs to be signed. |

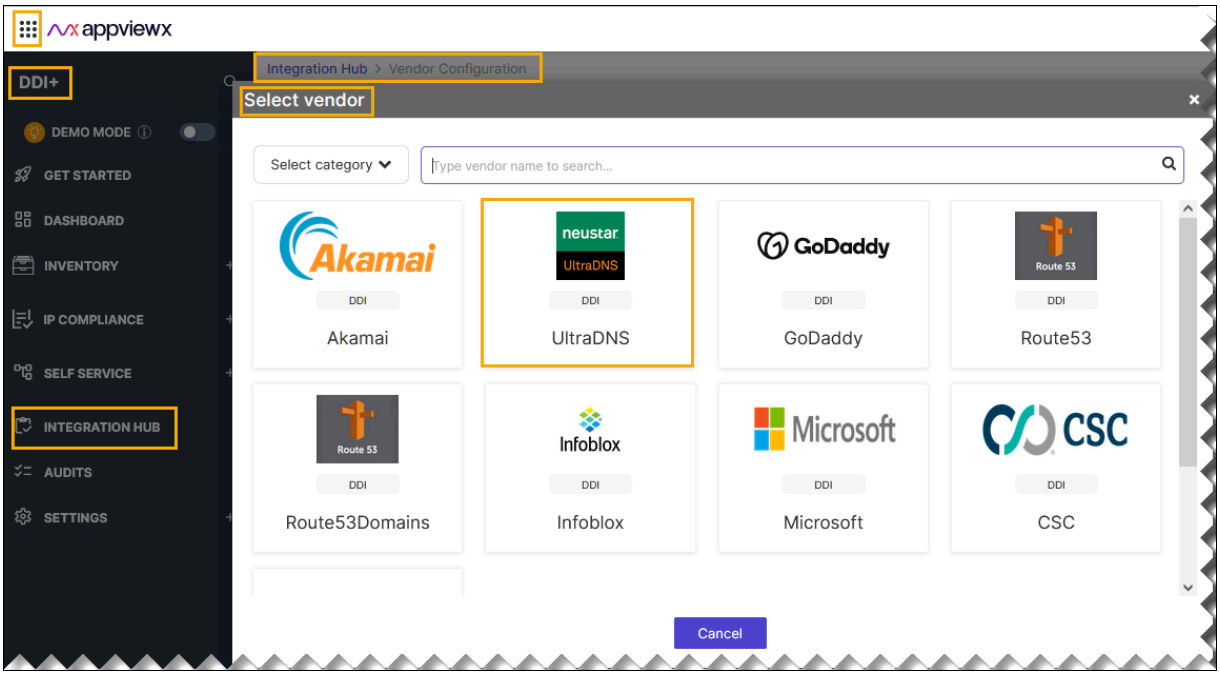
**: Mandatory fields*

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Config** toggle to add additional vendor configuration attributes.
7. Click **Finish**.

## Configuring UltraDNS

To configure UltraDNS:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **UltraDNS**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **OAuth 2.0** method of authentication selected by default. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Username** | Enter the valid username |

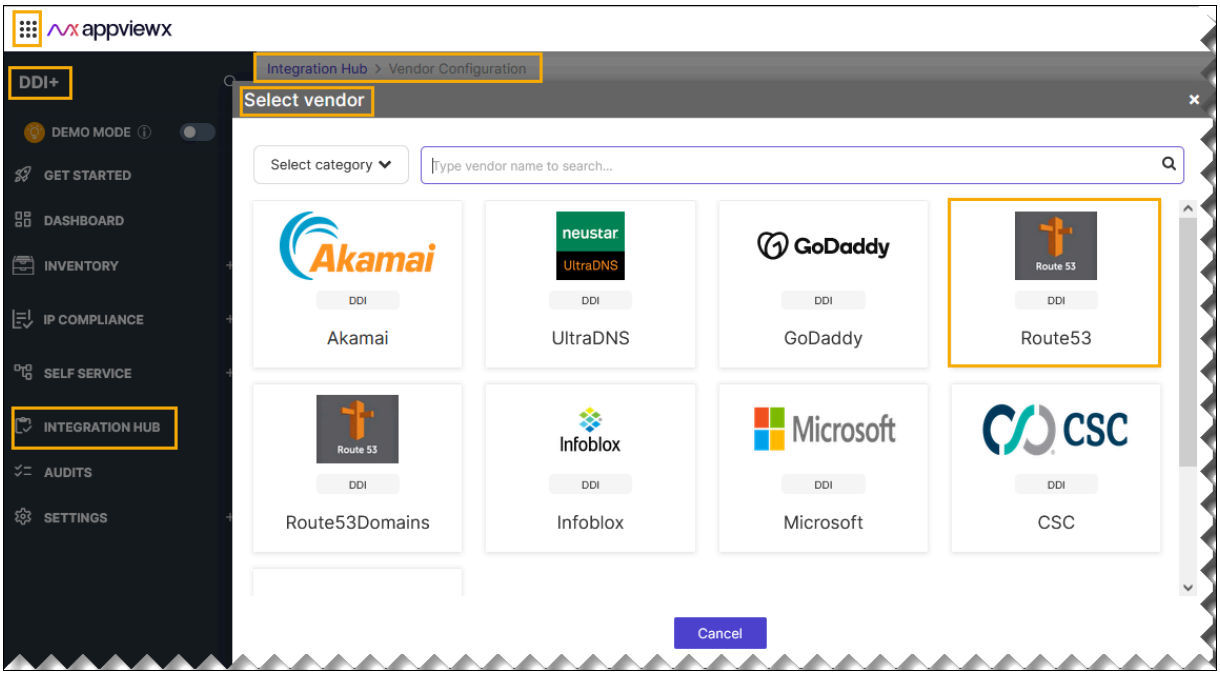
| Field | Description |
|---|---|
| ***Access Token URL** | Enter the authentication URL to obtain an access token to authenticate UltraDNS APIs. |
| ***Client ID** | Enter the unique Client ID provided by UltraDNS. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Password** | Enter the valid password. |
| ***Account Name** | Enter the UltraDNS account name for API integration. |
| ***Client Secret** | Enter the client secret given provided by UltraDNS. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Config** toggle to add additional vendor configuration attributes.
7. Click **Finish**.

## Configuring Route53

To configure Route53:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Route53**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **AWS signature** method of authentication selected by default. |
| ***Access Key** | Enter the Access Key provided by route53. |
| ***AWS Region** | Enter the region which is receiving the request. |

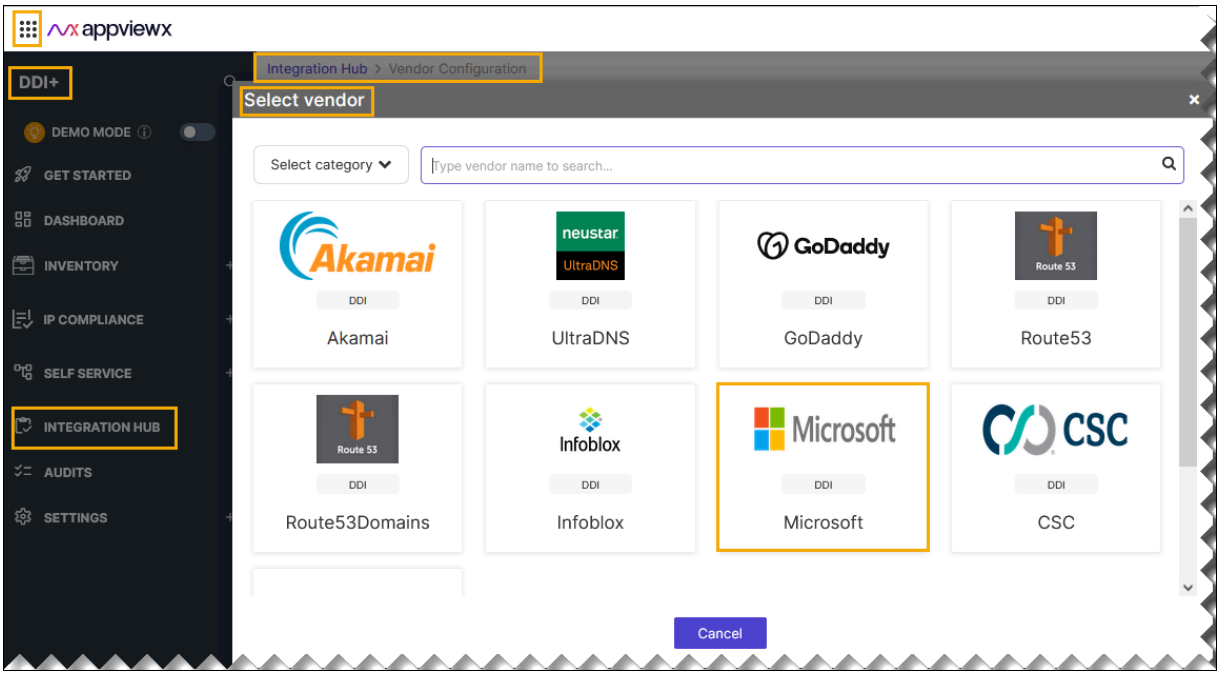
| Field | Description |
|---|---|
| **Session Token** | Enter the session token which is only required when using temporary security credentials. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol |
| ***Secret Key** | Enter the Secret Key provided by route53. |
| ***Service Name** | This field is filled by default. The service which is receiving a request. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advance Config** toggle to add additional vendor configuration attributes.
7. Click **Finish**.

## Configuring Microsoft

To configure Microsoft:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.



2. On the **Select Vendor** page, click **Microsoft**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

   The following table describes the various fields in this section:

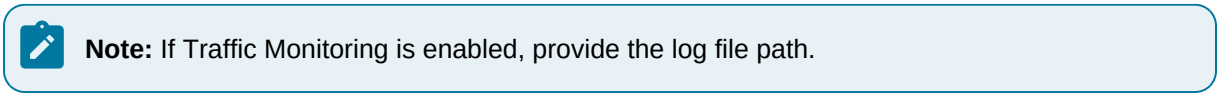
| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **Basic Auth** method of authentication selected by default. |
| ***Username** | Enter the valid user name. |
| **AD Account** | Enable if the provided user credentials correspond to an Active Directory (AD) user. Otherwise, disable for a local user. |
| ***Host Name** | Enter the valid hostname or IP address. |
| ***Passowrd** | Enter the valid password. |
| **Computer Names** | If AD Account is enabled, provide multiple computer names separated by commas. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. Enable the **Traffic Monitoring** button for parsing the DNS queries of the vendor.




7. Enter the Log **File Path** for the traffic monitoring.

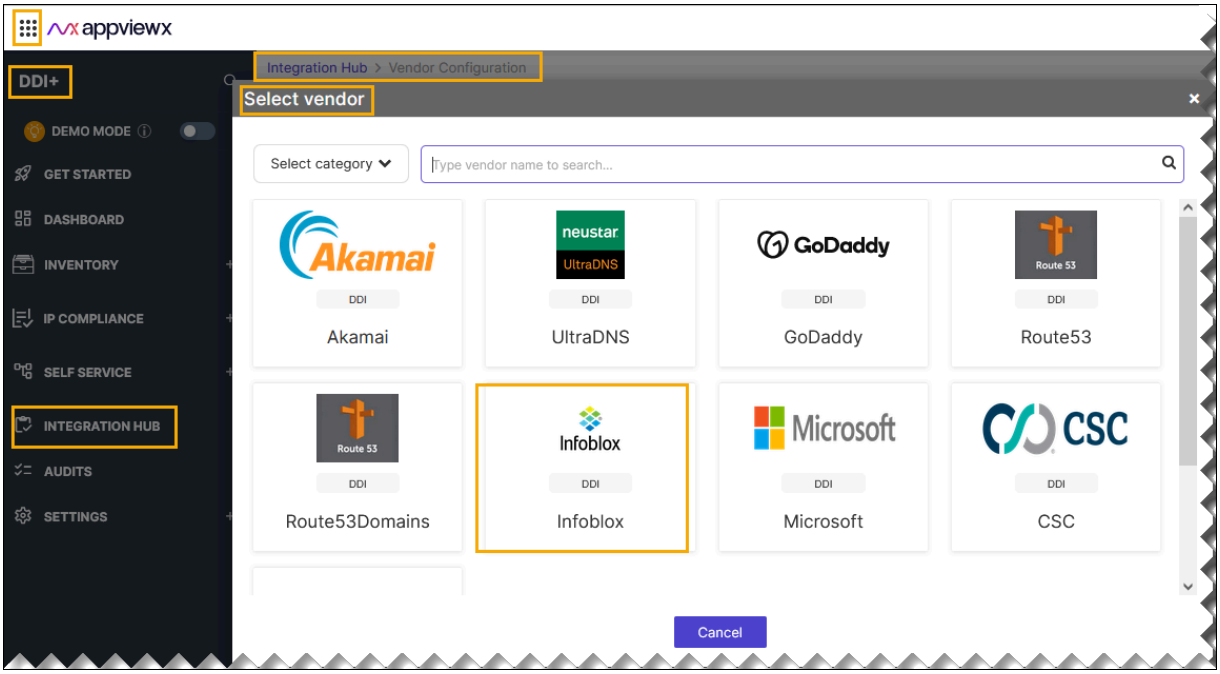
**Note:** To enable Traffic Monitoring in DDI+, it is necessary to obtain the debugging log from the Microsoft DNS server. The log file must be located in a shared folder, and user must have read access to this shared folder. This shared folder serves as the path through which the debugging log is retrieved for the Traffic Monitoring functionality in DDI+ platform.

8. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes if required.
9. Click **Finish**.

## Configuring Infoblox

To configure Infoblox:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Infoblox**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **Basic Auth** method of authentication selected by default. |
| ***Username** | Enter valid username. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Passowrd** | Enter the valid password. |
| **: Mandatory fields* | |

5. Enable **Sync IPAM** for parsing the IP Address Management (IPAM) data of the vendor.
6. Enable **Config sync** for parsing the vendor.
7. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes.


**Sample Schema**:


```
{
    "subnet": {
        "advanced_fields": [
            {
                "fieldName": "dynamic_hosts",
                "displayName": "Dynamic Hosts"
            },
            {
                "fieldName": "authority",
                "displayName": "Authority"
            },
            {
                "fieldName": "ddns_ttl",
                "displayName": "DNS update Time to Live"
            },
            {
                "fieldName": "discover_now_status",
                "displayName": "Discover Now Status"
            },
            {
                "fieldName": "vlans",
                "displayName": "Vlans"
```

```
                }
            ],
            "supernet": {
                "sync": true,
                "advanced_fields": [
                    {
                        "fieldName": "utilization",
                        "displayName": "Utilization"
                    }
                ]
            }
        },
        "ipv4address": {
            "advanced_fields": [
                {
                    "fieldName": "discover_now_status",
                    "displayName": "Discover Now Status"
                }
            ]
        },
        "ipam": {
            "classCLimit": 500,
            "classB1Limit": 4,
            "classB2Limit": 100,
            "ipPaginationLimit": 10000,
            "subnetPaginationLimit": 1000
        },
        "dns": {
            "recordsPaginationLimit": 1000,
            "zonesPaginationLimit": 1000,
            "zoneLimit": 500,
            "scriptApiLimit": 100
        },
        "custom_action": {
            "name": ""
        }
}
```

The following table explains the strings in the JSON schema:

| Strings | Description |
|---|---|
| **subnet > advanced_fields** | |
| dynamic_hosts | The total number of DHCP leases issued for a network refers to the count of unique IP addresses that have been dynamically assigned. |
| authority | The "authority" for a DHCP network typically refers to the entity responsible for managing and maintaining the DHCP server infrastructure. |
| ddns_ttl | The DNS update Time to Live (TTL) value of a DHCP network object. |
| discover _now_status | Current status of immediate discovery for this network. |
| discovered _bgp_as | Number of the discovered BGP AS. |
| discovered _vlan_id | Identifier of the discovered VLAN. |
| discovered _vlan_name | Name of the discovered VLAN. |
| discovered _vrf_description | Description of the discovered VRF. |
| discovered _vrf_name | Name of the discovered VRF. |
| discovered _vrf_rd | Route distinguisher of the discovered VRF. |

| Strings | Description |
|---|---|
| discovery _engine_type | Network discovery engine type. |
| total_hosts | Total number of DHCP addresses configured in the network. |
| vlans | List of VLANs assigned to Network. |
| **subnet > supernet > advanced_fields** | |
| utilization | The network utilization in percentage. |
| **ipv4address > advanced_fields** | |
| discover _now_status | Current status of immediate discovery for this address. |
| classCLimit | Number of Class C subnets to be parsed in a single child request.<br>**Note:** If this number is reduced, number of child workflows will increase. |
| classB1Limit | Number of class B1 (/16 to /19) subnets to be parsed in a single child request.<br>**Note:** If this number is reduced, number of child workflows will increase. |
| classB2Limit | No of class B2 (/20 to /23) subnets to be parsed in a single child request.<br>**Note:** If this number is reduced, number of child workflows will increase. |
| ipPagination Limit | Number of IPAddresses to be fetched in a single Infoblox ipv4 API call. |
| subnet Pagination | Number of Subnets to be fetched in a single Infoblox network API call. |

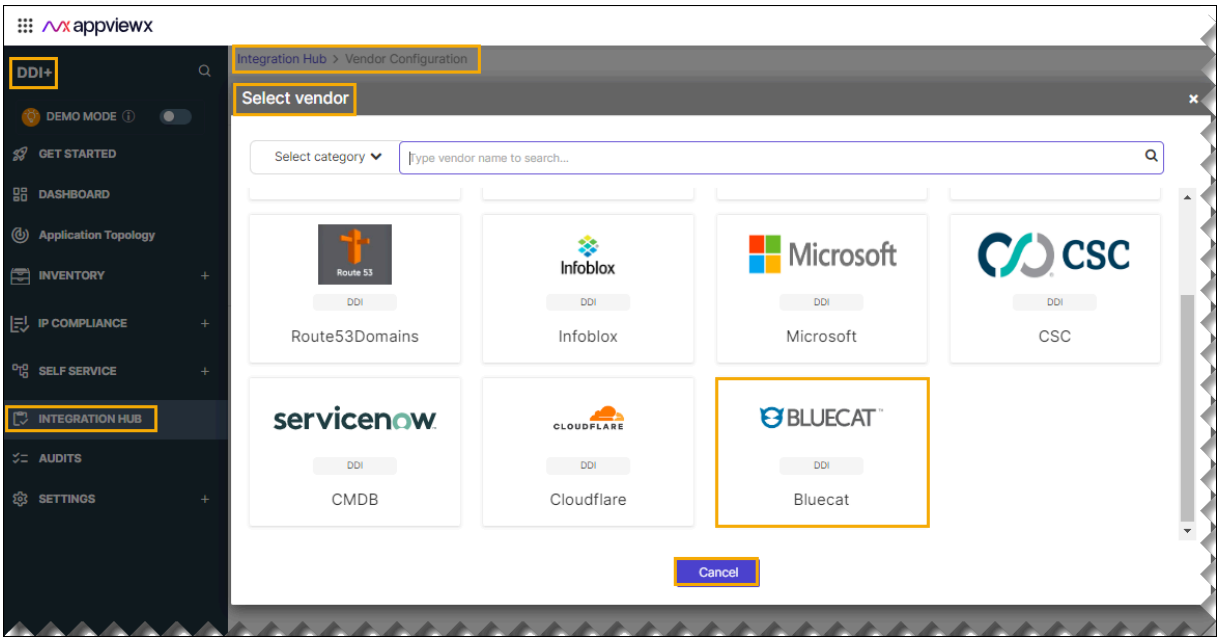
| Strings | Description |
|---|---|
| Limit | |
| records<br>Pagination<br>Limit | Number of Records to be fetched in a single Infoblox records API call. |
| zones<br>Pagination<br>Limit | Number of Zones to be fetched in a single Infoblox auth_zone API call. |
| scriptApiLimit | Number of records APIs to handle in a single script call. |
| custom<br>_action > name | Custom workflow name to be triggered after the Infoblox sync is complete |
| **: Mandatory fields* | |

8. Select **CMDB Source** from the dropdown list to correlate IPAM data with the CMDB.
9. Click **Finish**.

## Configuring Bluecat

To configure Bluecat:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Bluecat**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **Basic Auth** method of authentication selected by default. |
| ***Username** | Enter valid username. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Password** | Enter the valid password. |

| Field | Description |
|---|---|
| ***Access Token URL** | Enter the authentication URL to obtain an access token to authenticate Bluecat APIs. For example, https://%3Ctest%3E.appviewx.net/Services/REST/v1/login |
| ***API Version** | Select the preferred API version from the dropdown list. By default **v1** is selected. |
| **: Mandatory fields* | |

5. Enable **Sync IPAM** for parsing the IP Address Management (IPAM) data of the vendor.
6. Enable **Config sync** for parsing the vendor.
7. Enable **Sync DNS** for parsing the vendor.
8. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes.


**Sample Schema**:

```
{
 "ipam": {
  "ipPaginationLimit": 10000,
  "subnetPaginationLimit": 1000,
  "asyncRequestCount": 4
 },
 "dns": {
  "recordsPaginationLimit": 1000,
  "asyncRequestCount": 4
 },
 "custom_action": {
```

```
 "name": ""
 }
}
```

The following table explains the strings in the JSON schema:

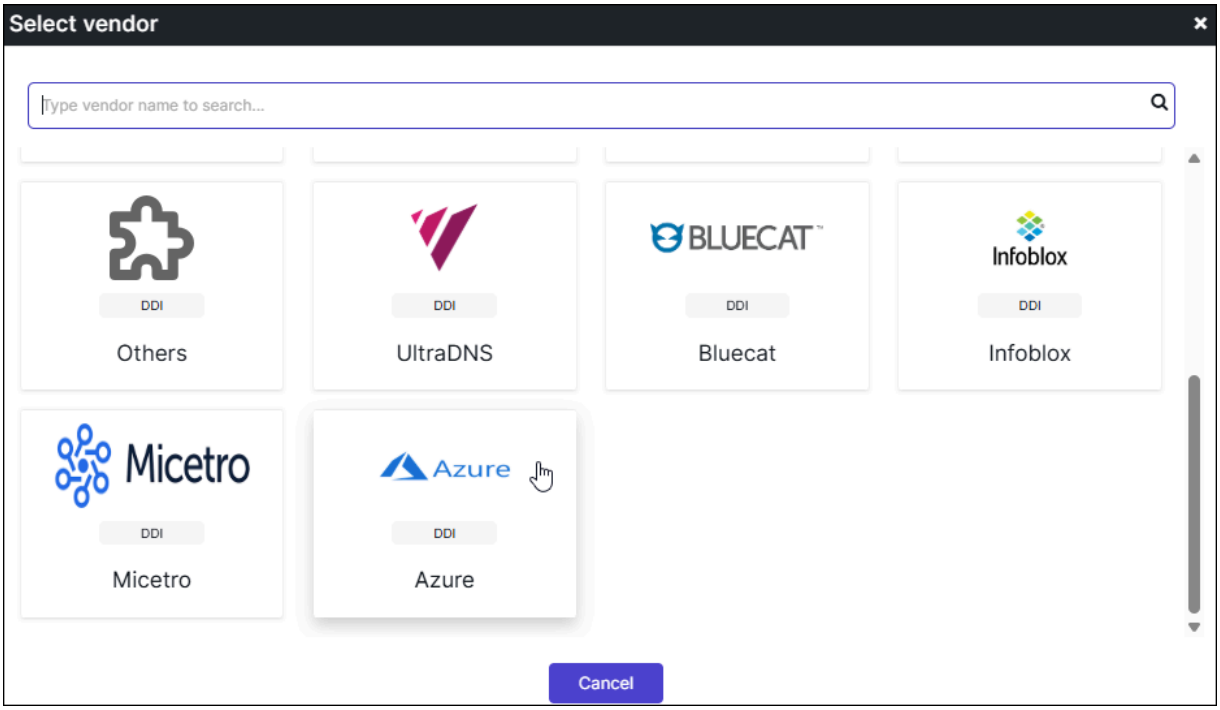
| Strings | Description |
|---|---|
| dns | The DNS update Time to Live (TTL) value of a DHCP network object. |
| recordPaginationLimit | CMDB Data Fetch Limit per Vendor API Call (For example, ServiceNow CMDB API Limit).<br>**Note:** This API pagination limit specifies the number of CMDB records that can be retrieved in a single API call from ServiceNow. |
| asyncRequestCount | AppViewX initiates parallel calls to devices to synchronize data. The asyncRequestCount specifies the number of simultaneous calls AppViewX can make at any given time. |
| ipPaginationLimit | Number of IPAddresses to be fetched in a single Infoblox ipv4 API call. |
| subnetPaginationLimit | Number of Subnets to be fetched in a single Infoblox network API call. |
| asyncRequestCount | AppViewX initiates parallel calls to devices to synchronize data. The asyncRequestCount specifies the number of simultaneous calls AppViewX can make at any given time. |
| custom_action > name | Custom workflow name to be triggered after the Infoblox sync is complete |
| *: Mandatory fields | |

9. Select **CMDB Source** from the dropdown list to correlate IPAM data with the CMDB.
10. Click **Finish**.

## Configuring Micetro

To configure Micetro:

1. Go to **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **Micetro**.
   The **Vendor Configuration** page is displayed.
3. Under the **General** section, enter or select the required field information.
   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. Click **Next**.

   You will be redirected to the **Credentials** page.

5. Under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Auth Type** | Displays the **Basic Auth** method of authentication selected by default. |
| ***URL** | Enter the URL of the vendor with the HTTPS/HTTP protocol. |
| ***Username** | Enter valid username. |
| ***Password** | Enter the valid password. |
| **: Mandatory fields* | |

6. Click **Next**.

   You will be redirected to the **Configurations** page.

7. Under the **Configurations** section, enter or select the required field information.

   a. Enable toggle to **Use Proxy**.

   > **Note:** Before enabling, please add proxy details under **Menu** -> **Settings** -> **General** -> **Proxy**.

   b. Enable **Config Sync** for parsing the vendor.

   c. Enable **Enable Advanced Config** toggle to add additional vendor configuration attributes.


8. Click **Finish**.

   The **Vendor configurations saved successfully** message is displayed.

## Whats Next

To view status of the configuration, click View Status.

## Onboarding CMDB

Integrate CMDB to discover IP assets and ensure compliance with IPAM and load balancer systems within the DDI+ platform.

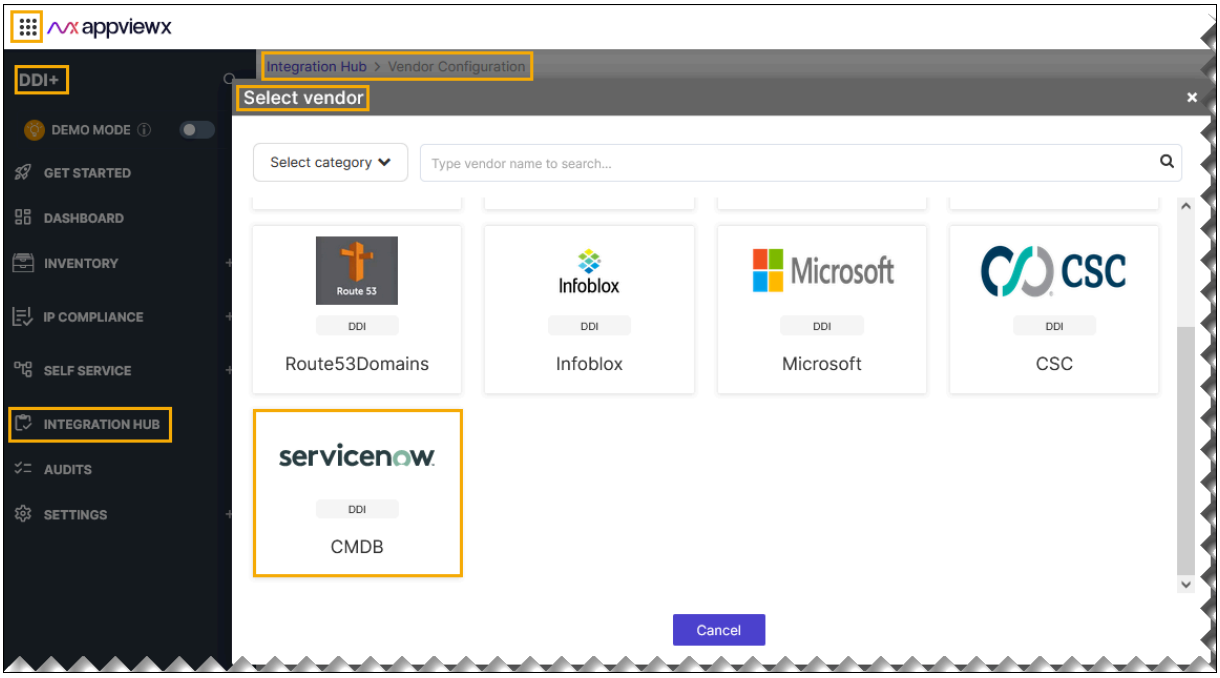
- Configuring ServiceNow

## Configuring ServiceNow

To configure CMDB and sync the IP assets from the CMDB. DDI+ platform must be configured with tables in CMDB which have IP asset information. IP asset information and its associated data can be present in one or multiple tables.

To configure ServiceNow:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.




2. On the **Select Vendor** page, click **ServiceNow**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

The following table describes the various fields in this section:

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| **: Mandatory fields* | |

4. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

| Field | Description |
|---|---|
| **Auth type** | Displays the **Basic Auth** method of authentication selected by default. |
| ***Username** | Enter valid username. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| ***Password** | Enter the valid password. |
| **: Mandatory fields* | |

5. Enable **Config sync** for parsing the vendor
6. On the **Vendor Configuration** page, under the **Configurations** section, turn on the **Enable Advanced Config** toggle to add additional vendor configuration attributes.

```
{
    "cmdbSource": {
        "tables": [
            {
                "type": "ASSET",
                "table_name": "cmdb_ci_ip_address",
                "url": "/api/now/table/cmdb_ci_ip_address",
                "fields": [
                    {
                        "fieldName": "ip_address",
                        "displayName": "IP Address",
                        "unique": true
                    },
                    {
                        "fieldName": "fqdn",
                        "displayName": "FQDN"
                    },
                    {
                        "fieldName": "asset_tag",
                        "displayName": "Asset Tag"
                    },
                    {
                        "fieldName": "sys_created_by",
                        "displayName": "Created By"
```

**Sample Schema**:

```
{
"avxPaginationLimit": 10000,
"paginationLimit": 10000,
"deltaSync": true,
"orphanIP": {
"condition": "ALL",
"dataFields": [
"ITAM ID",
"Owned By"
]
},
"tables": [
{
"type": "ASSET",
"table_name": "cmdb_ip_address",
"url": "/api/now/table/cmdb_ci_ip_address",
"fields": [
{
"fieldName": "ip_address",
"displayName": "IP Address",
"unique": true
},
```

```
{
"fieldName": "asset_tag",
"displayName": "ITAM ID"
},
{
"fieldName": "subcategory",
"displayName": "Sub Category"
},
{
"fieldName": "short_description",
"displayName": "Technology Stack"
},
{
"fieldName": "category",
"displayName": "Category"
},
{
"fieldName": "operational_status",
"displayName": "Operation Status"
},
{
"fieldName": "owned_by",
"displayName": "Owned By"
},
{
"fieldName": "business_unit",
"displayName": "Business Unit"
},
{
"fieldName": "install_status",
"displayName": "Installation Status"
},
{
"fieldName": "vendor",
"displayName": "Vendor"
}
]
```

```
},
{
"type": "META",
"table_name": "cmdb_ci_service_discovered",
"url": "/api/now/table/cmdb_ci_service_discovered",
"fields": [
{
"fieldName": "operational_status",
"displayName": "Operational Status"
},
{
"fieldName": "number",
"displayName": "Number"
},
{
"fieldName": "used_for",
"displayName": "Used for"
},
{
"fieldName": "process_status",
"displayName": "Process Status"
},
{
"fieldName": "service_status",
"displayName": "Service Status"
},
{
"fieldName": "busines_criticality",
"displayName": "Business Criticality"
},
{
"fieldName": "managed_by",
"displayName": "Managed By"
},
{
"fieldName": "vendor",
"displayName": "Vendor"
```

```
},
{
"fieldName": "assigned_to",
"displayName": "Assinged To"
},
{
"fieldName": "asset_tag",
"displayName": "Asset Tag",
"correlationField": "ITAM ID"
},
{
"fieldName": "install_status",
"displayName": "Installation Name"
},
{
"fieldName": "name",
"displayName": "App Service Name"
},
{
"fieldName": "location",
"displayName": "Location"
}
]
}
]
}
```


The following table explains the strings in the JSON schema:

| Strings | Description |
|---|---|
| avxPaginationLimit | CMDB Data Fetch within AppViewX.<br><br>**Note:** This pagination limit specifies the number of records processed in each pagination cycle, crucial for establishing a correlation within AppViewX between CMDB and IP data. |

| Strings | Description |
|---|---|
| paginationLimit | CMDB Data Fetch Limit per Vendor API Call (For example, ServiceNow CMDB API Limit).<br><br>**Note:** This API pagination limit specifies the number of CMDB records that can be retrieved in a single API call from ServiceNow. |
| deltaSync | This is a boolean value true/false.<br><br>True: After the initial synchronization, AppViewX will only sync the changes that have been updated in the CMDB since the last configuration fetch.<br><br>False: At config sync all the CMDB tables data will be fetched. |
| orphanIP | OrphanIP setting is to identify orphan IPs based on certain conditions. |
| condition | ALL - All Specified fields should have data else the IP will be considered as orphan.<br><br>ANYONE - Any one specified field should have data else the IP will be considered as orphan. |
| dataFields | List of CMDB Data Fields need to be validated for Orphan IP Logic; Enter the displayLable name for the fields. |
| tables | List of CMDB Tables data need to be synced. |
| type | Type of Table Data:<br>• ASSET - CMDB Asset Data<br>• META - Meta Data of Asset. |
| table_name | Table name of the data needs to be synced. |
| url | URL to fetch the data from the given asset table. |
| fields | List of field names from the CMDB table to synced . |
| fieldName | Field name from CMDB Table data. |
| displayName | Display name for the field in AppViewX. |

| Strings | Description |
|---|---|
| unique | Whether field must be considered for data uniqueness or not. The possible value True (or) False. |
| correlationField | This configuration specific to CMDB meta data tables config. Link field data between asset table and meta table. |
| *: Mandatory fields | |

7. Click **Finish**.

## Configuring Other Vendor

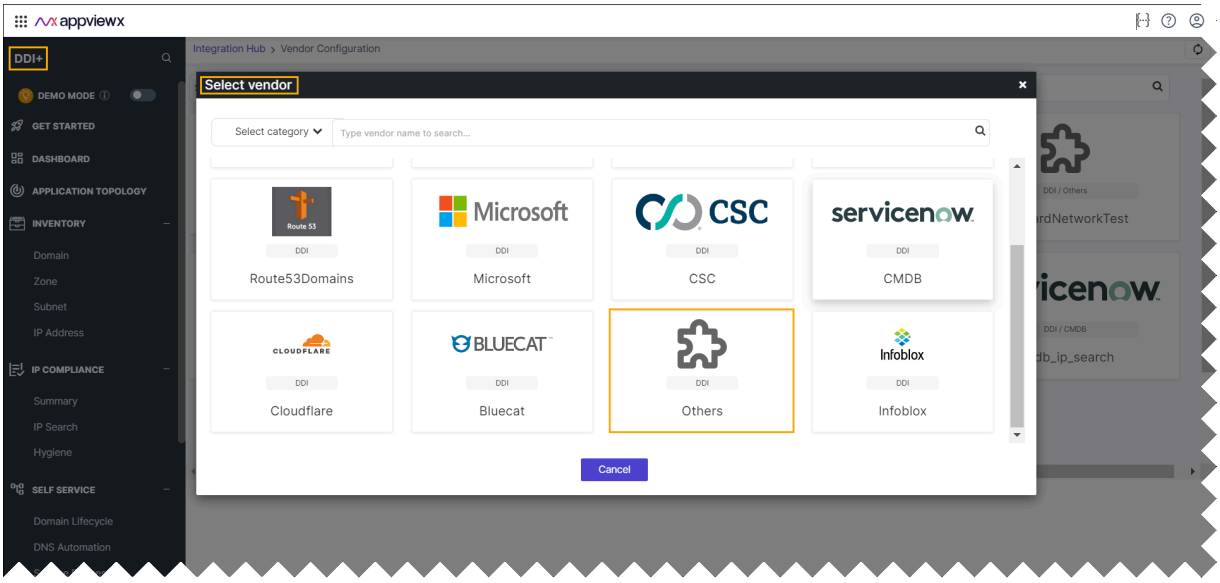
Integrate custom sources that maintain IP address details with AppViewX to sync IP-related information into the database. This IP data can then be correlated with DNS providers, IPAM information, ServiceNow, and other systems.

**Prerequisites**:

Before you configure other vendor, ensure you created a custom workflow to sync the data from the vendor into DDI+ custom collection.

To configure other vendor:

1. Go to **DDI+** > **INTEGRATION HUB**, and then click **Add new vendor**.
   The **Select vendor** page is displayed.



2. On the **Select Vendor** page, click **Others**.
3. On the **Vendor Configuration** page, under the **Information** section, enter or select the required field information.

   The following table describes the various fields in this section:

**General - Field and Description Table**

| Field | Description |
|---|---|
| ***Name** | Enter a unique name to identify the vendor account which is being configured. |
| **Description** | Enter a description for the purpose of configuring this vendor, if required. |
| **Data center** | Select a data center from the options available in the dropdown list. |
| ***Vendor** | Enter the vendor name. |
| **: Mandatory fields* | |

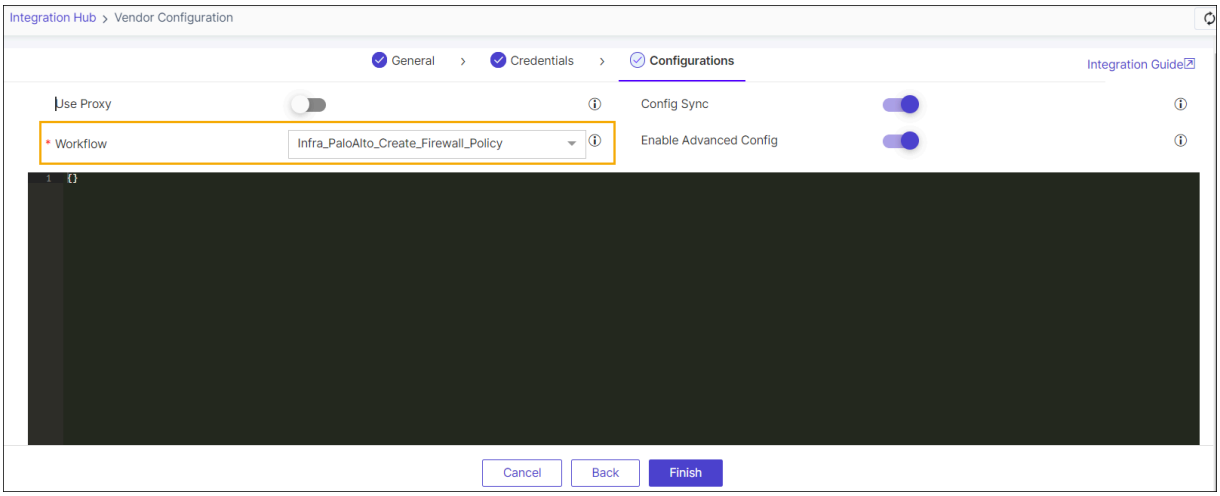
4. Click **Next**.
5. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the required field information.

   The following table describes the various fields in this section:

**Credentials - Field and Description Table**

| Field | Description |
|---|---|
| ***Auth type** | Displays the **Basic Auth** method of authentication selected by default. Select a desired authentication type from the dropdown list.<br><br>**Note:** Based on the Auth type selection, you will need to enter the the auth-related fields. |
| ***URL** | Enter API URL for the vendor with the HTTPS/HTTP protocol. |
| **: Mandatory fields* | |

6. Click **Next**.
7. On the **Vendor Configuration** page, under the **Configurations** tab, select a custom workflow from the **Workflow** dropdown list.




**Note:** If the **Enable Advanced Config** toggle is turned on, **BlueCat and Infoblox** vendor sync integrations for */4* **and larger subnets** can be excluded by specifying the subnet details in the `"skipSubnets": []` array.

This workflow initiates the process of adding data into DDI+.

8. Click **Finish**.

   It takes a while sync the data into DDI+. You can view the data in IP Search.

**Note:** You need to add an entry for the custom source to the `ddi_settings_collection` within the `IP_Search_Settings` document in the sources. This will enable data synchronization in IP Search.

## Whats Next

IP Search

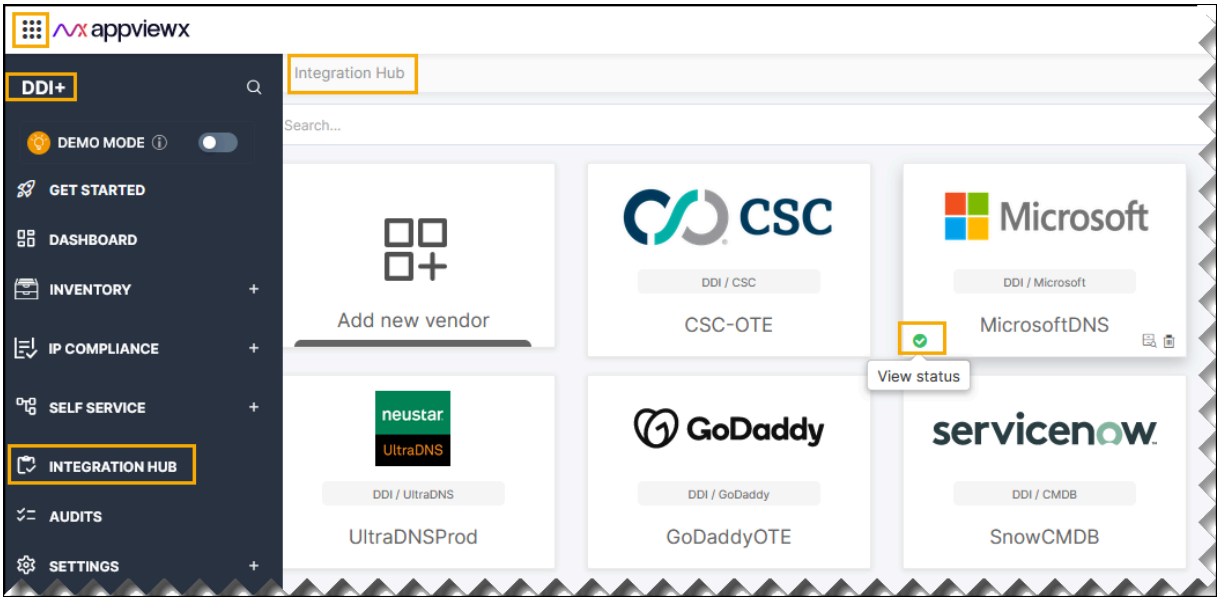
## Integration Hub Vendor Actions

For each vendor on-board in the integration hub, the following actions can be performed when you hover over the vendor tile.

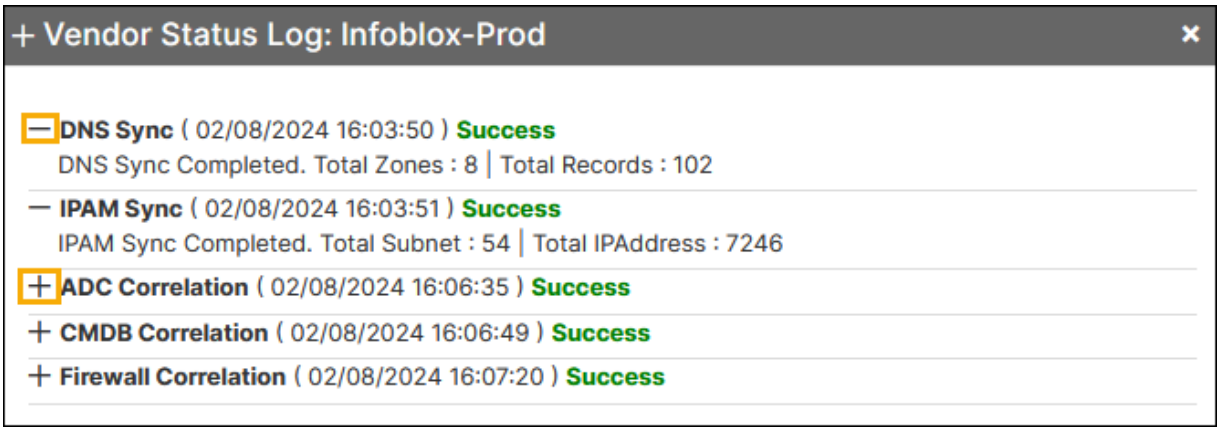
### Viewing Status

To view status of the configuration sync when a vendor is on-boarded or triggered manually, perform the following steps.

1. Go to **DDI+** > **INTEGRATION HUB**, and then click the **View status** icon on the vendor.




The Vendor Status Log window is displayed.

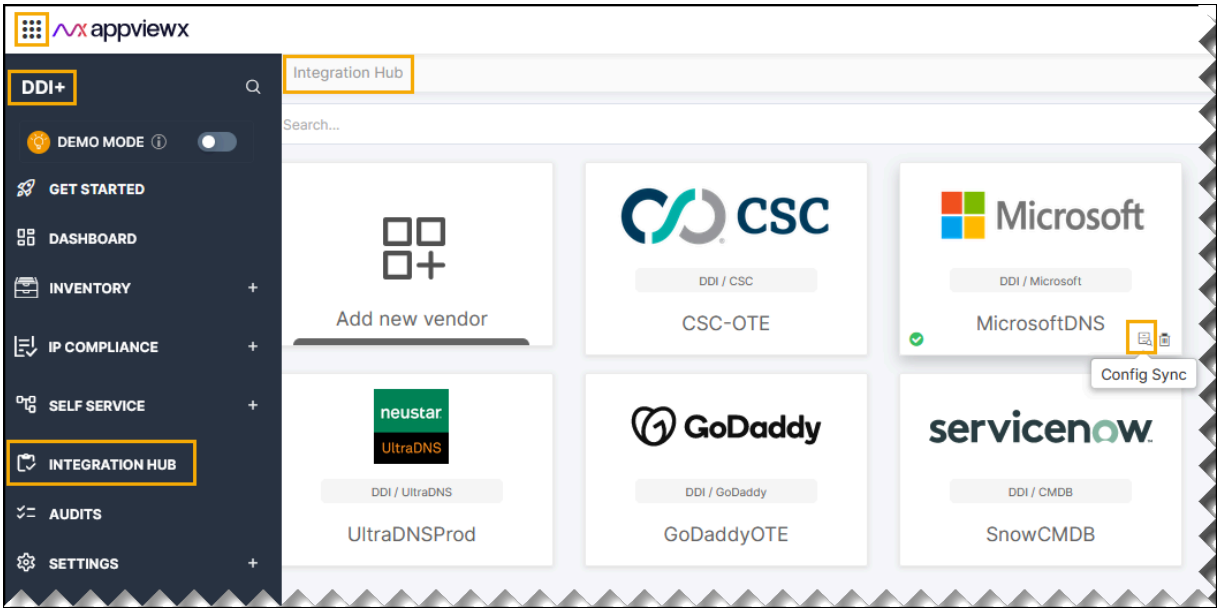



2. Click the (**+**) maximize icon that you want to view the status log.
3. Click the (**-**) minimize icon that you want to view the status log.

## Triggering Config Sync

Users can manually trigger the config sync by clicking the **Config sync** button. To trigger the config sync, perform the following steps.

1. Go to **DDI+** > **INTEGRATION HUB**, and then click the **Confg sync** icon on the vendor.

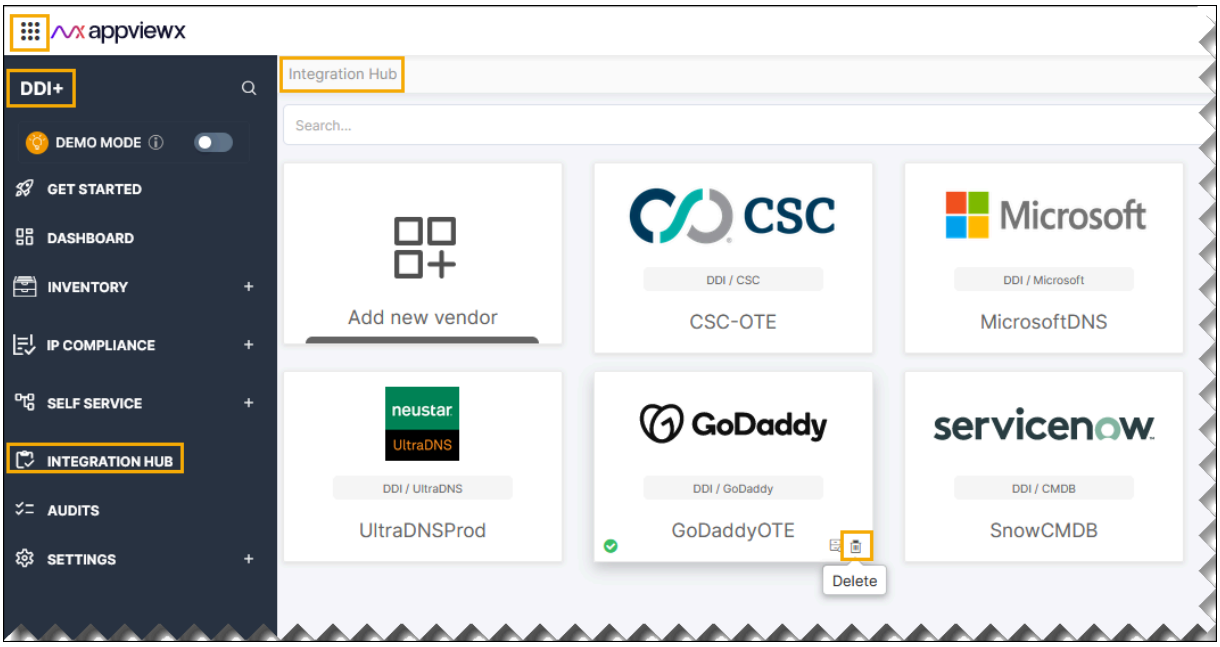



2. The pop-up message is displayed as **Operation performed successfully**.

## Deleting Vendor

To delete the vendors and its associated configuration from AppViewX, perform the following steps.

1. Go to **DDI+** > **INTEGRATION HUB**, and then click the **Delete** icon on the vendor.




2. The pop-up message is displayed as **Do you want to delete the vendor configuration ?**.

3. Click **Ok**
4. The pop-up message is displayed as **Operation performed successfully**.

# Audits

This section displays all the audit logs related to DDI+. Different severity levels are displayed for the audit logs within this section.

# Settings

The DDI+ settings enable you to customize the Extensible Attributes feature, which are reflected in the dashboard interface.

- Extensible Attributes.
- Extensible Attributes Settings

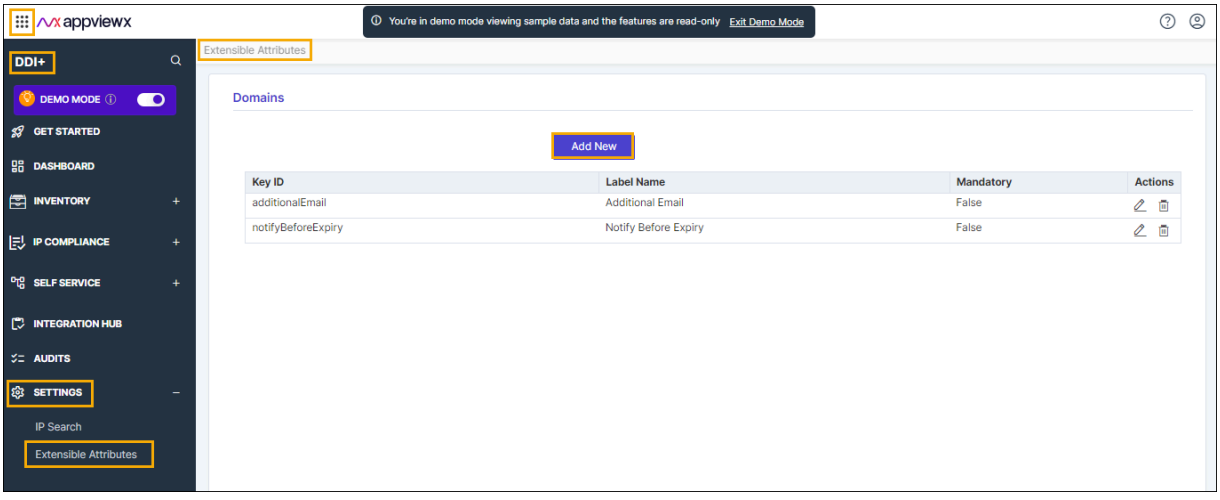
## Extensible Attributes Settings

Extensible attributes are additional attributes that organizations may need to record as part of their domains.

To configure the Extensible Attribute:

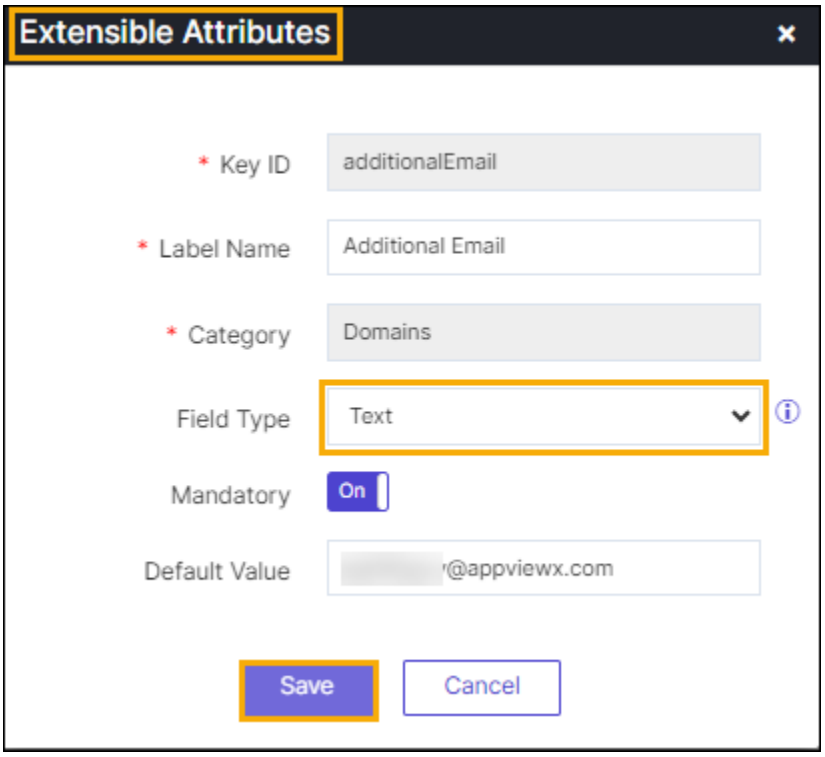
1. Go to **DDI+** > **SETTINGS**, and then click **Extensible Attributes**.

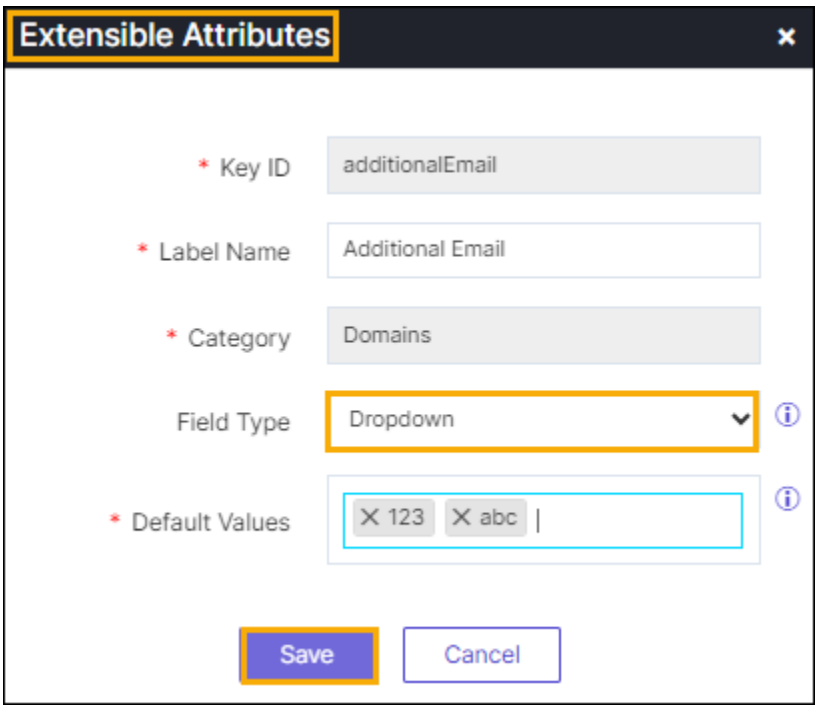
   The **Domains** page is displayed.



2. In the **Domains** section, click the **Add New** button.

   The **Extensible Attribute** window is displayed.




   The following table describes the various fields in this section.

| Field | Description |
|---|---|
| ***Key ID** | Enter the valid key ID. |
| ***Label Name** | Enter the name of the label. |
| ***Category** | By default, the **Domains** category is displayed. |
| **Field Type** | Select the desired extensible attribute type form the dropdown list. The available types are:<br>• Text<br>• Dropdown. |
| **Mandatory** | Move the radio button for **On** or **Off**.<br>**Note:** This option will be enabled when the field type is selected as Text. |
| ***Default Value** | Enter the valid Email ID. |
| **: Mandatory fields* | |

3. Click **Save**.

# Chapter 3: DDI+ API Guide

This guide provides information about the AppViewX exposed APIs intended for use in **DDI+** actions.

### Best Practices for Working with the AppViewX API

- **Use appropriate HTTP methods**

  Ensure that the correct HTTP method is used for each operation (e.g., GET for retrieval, POST for creation).

- **Handle errors gracefully**

  Implement proper error handling in your application to manage API responses.

- **Use secure storage**

  Store access tokens securely and avoid hardcoding them in your application code.

- **Implement pagination**

  For endpoints that return large datasets, implement pagination using limit and offset parameters.



## Understanding the AppViewX DDI+ API

The AppViewX DDI+ API provides design and implementation of a solution for retrieving IP trace data from multiple sources through a unified, generic API. This section covers how to make requests, handle responses, and understand the structure of the API.

- API 1: Retrieves a list of data sources that contain traces for a given IP address.
- API 2: Retrieves detailed IP trace information from a specified source identified by **API 1**.

### RESTful HTTPS Requests

The DDI+ API uses RESTful principles, leveraging standard HTTP methods to interact with resources. All requests must be made over HTTPS to ensure security.

| Type | Description |
|---|---|
| **GET** | GET requests, retrieve resource representation/information only and not to modify it. |
| **POST** | POST APIs create new subordinate resources. For example, a file is subordinate to a directory containing it or a row is subordinate to a database table. In terms of REST, POST methods are used to create a new resource into the collection of resources. |
| **PUT** | PUT APIs are used to update existing resources (if a resource does not exist then API may decide whether to create a new resource or not). |
| **DELETE** | DELETE APIs are used to delete resources (identified by the Request-URI). |

## Requests

All API endpoints are accessed via the following base URL. The base URL is built in the same way by the following structure:

```
http://<IP/HostName/TenantName>:<GWPORT>/avxapi/<Endpoint>?<gwsource>
```

The explanation has been added to all APIs in the Reference section.

**Understanding the sample URL:**

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

## Request Structure

All endpoints accept a request structure that should consist of JSON formatted data. To ensure the request is accepted, set the header **Content-Type: application/json**.

The following example shows a request to add a resource:

```
{
"payload": {
"name": "resource_1",
"description": "This is a sample resource."
}
}
```

## Response Structure

The Content-Type of the response is typically determined by the Content-Type header, and for most endpoints, it will be application/json. All requests that reach the server, regardless of the response code, will retrieve a response body. A successful request will contain a body with the requested information, for example:

```
https://appviewxapi.com/avxapi/resource?gwsource=external
```

Returns the following JSON structure that a resource is added:

```
{
"response": "Resource added successfully",
"message": "Resource added successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

### Description of Server Responses

| HTTP Code | Response Message |
|---|---|
| **200** OK | The request was successful (some API calls may return 201 or 202 instead). |
| **400** Bad Request | The request is not understood or required parameters are missing. |
| **401** Unauthorized | Authentication failed or the user doesn't have permissions for the requested operation. |
| **409** Forbidden | Access denied. |
| **404** Not Found | Resource not found. |
| **429** Too many requests | The number of requests to the service has crossed the threshold. |
| **503** Service unavailable | The client cannot communicate with the service. |
| **504** Gateway timeout | The given request has exceeded the expected time. |

### URI Scheme

- **Host :** {url}
- **BasePath :** /avxapi
- **Schemes :** HTTPS
- **URL :** https://{url}/avxapi

### Types of Accounts in AppViewX

There are two types of accounts in AppViewX:

- **User Accounts**: These are used by actual users.
- **Service Accounts**: These are used by system services such as web servers, automation tools, and so on.

AppViewX recommends using a Service Account for accessing APIs from automation tools. Service Accounts are supported with oAuth standard for a more secure and standard way of accessing APIs.

**Note:** AppViewX supports both User Account and Service Account for accessing APIs.

# Authentication Using a User Account

For accessing APIs, you can login via two types of accounts:

- User account

  A **User account** represents an individual person interacting with the application or the system. User accounts are used for accessing the system on behalf of a user.

  For accessing APIs with a user account, you need to get the session ID by providing a username and password in the login API. This session ID can then be used for accessing other APIs.

  **Note:** You can also use the username and password in all API calls instead of the sessionId. However, this is not recommended.

- Retrieve session ID using login API
- Using Session ID for further API calls

## Retrieve session ID using login API

This API used to retrieve the session ID using the login API for secure authentication and access to system resources.

### Before you begin

- Make sure you have valid login credentials (Username and Password) for accessing the system.
- You cannot use OAuth credentials (Client ID and Client Secret) for login.
- To access the APIs using the service token, use the API with the Service Account.

### Request Structure

| | |
|---|---|
| **Endpoint** | /login |
| **Type** | POST |
| **Sample URL** | https://<IP/HostName/TenantName>:<GWPORT>/avxapi/login?gwsource=external<br><br>To understand the elements of the sample URL, click here. |
| **Headers** | |
| **Content-Type** | application/json |

| | |
|---|---|
| **Request timeout period** | 15 minutes |

**Input Parameters**

| Name | Description |
|---|---|
| username<br>*Header* | (Mandatory) Use login name of the user.<br>**Type:** String<br>**Example:** "admin" |
| password<br>*Header* | (Mandatory) Password for the username.<br>**Type:** String<br>**Example:** "AppViewX@123" |
| otp<br>*Header* | (Mandatory only if MFA is enabled) If MFA is enabled, enter the OTP received on your registered email ID in the header.<br>Multifactor authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a resource<br>If MFA is enabled, and you try to login with only the username and password, you will get the following error upon execution of the API: **MFA is enabled. We have sent an OTP to your email ID: aaa********r@appviewx.com**. In this case, ensure that the OTP is included in the header and try logging in again.<br>**Type:** String<br>**Example:** "OTP : **609700**" |
| Content-Type<br>*Header* | (Mandatory) The parameter should be set to `application/json` to specify the nature of the data in the payload.<br>**Type:** String<br>**Example:** "application/json" |

**Input Parameters (continued)**

| Name | Description |
|---|---|
| gwsource<br>*Query* | (Mandatory) Source from which the request is triggered. The values can be:<br>• web<br>• external<br><br>**Type:** String |

## Response Structure

- **Status Code:** 200 Ok
- **Message:** Login Successful
- **Headers:**
  - **Content-Type:** application/json

**Response Parameters**

| Name | Description |
|---|---|
| response | The response contains the attributes needed to retrieve the session ID. |
| message | Success message or failure description in case of error. |
| appStatusCode | Application specific status code for the response. Will be non-null for failure response. |
| tags | More info in case of failure response. |

| Name | Description |
|---|---|
| status | Indicates the overall status of the response. The values can be:<br>• SUCCESS<br>• FAILURE |
| appStatusCode | An application-specific status code, if applicable. |
| statusDescription | Description of the status, if available. |
| sessionId | Unique identifier for the session. |

| Name | Description |
|---|---|
| lockDownPeriod | Number of login attempts remaining. |
| termsAccepted | |
| passwordExpiryMsg | |
| emailId | |

## Status Codes

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 200 OK | NA | Login successful |
| 400 Bad request | ACCT_AUTH_001 | Username or password cannot be null or empty. |
| 401 Unauthorized | ACC_AUTH_022 | Login failed. Invalid credentials. |
| 401 Unauthorized | ACC_AUTH_006 | Login failed. Invalid credentials. |

## Sample Request/Response

### Use Case

Login to the application with a username and password.

### Request URL

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/login?gwsource=external
```

### Request Payload

```
{}
```

### Sample Response


```
{
    "response": {
        "status": "SUCCESS",
        "appStatusCode": null,
        "statusDescription": null,
        "sessionId": "avx~~c73a4f56-f4ab-4cdf-aadf-6d90bf406077",
        "authCode": null,
        "lockDownPeriod": 15,
        "emailId": null,
        "termsAccepted": true,
```

```
        "passwordExpiryMsg": ""
    },
    "message": "Login successful.",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


## What's Next

- **Using Session ID for further API calls**

## Reference

**Understanding the sample URL:**

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

## Using Session ID for further API calls

The sessionID retrieved using the login API can be used in the header for making further API calls.

**In this section, as an example, we are using the session ID with the API call for adding a role.**

### Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

### Request Structure

| | |
|---|---|
| **Endpoint:** | `/role` |
| **Type:** | `POST` |
| **Sample URL:** | `https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?&gwsource=external`<br><br>To understand the elements of the sample URL, click here. |
| **Headers:** | |
| **Content-Type:** | application/json |

**Input Parameters**

| Name | Description |
|---|---|
| sessionId<br><br>*Header* | (Mandatory) Use session ID retrieved from login API, if username and password are not provided.<br><br>**Type:** *String*<br><br>**Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813" |
| gwsource<br><br>*Query* | (Mandatory) Source from which the request is triggered. The values can be:<br><br>• web<br>• external<br><br>**Type:** *String* |
| Payload | (Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section. |

**Input Parameters (continued)**

| Name | Description |
|---|---|
| *String* | |

## Payload

| Name | Description |
|---|---|
| name | (Mandatory) Name of the role to be added. |
| *String* | **Example:** "role_1" |
| description | (Optional) Description of the role to be added. |
| *String* | **Example:** "Adding a new role" |

## Response Structure

- **Status Code:** 201 Created
- **Message:** Role added successfully
- **Headers:**
  - **Content-Type:** application/json

**Response Parameters**

| Name | Description |
|---|---|
| response | Contains the response attributes for role added successfully. |
| message | Success message or failure description in case of error. |
| appStatusCode | Application specific status code for the response. Will be non-null for failure response. |
| tags | More info in case of failure response. |

## Status Codes

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 201 Created | null | Role added successfully. |

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 409 Conflict | ACCT_RO_002 | Role name already exists |
| 400 Bad Request | VALIDATION_ERROR_0004 | 'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty. |
| 400 Bad Request | ACCT_RO_015 | Role name invalid. |

## Sample Request/Response

### Use Case

Using the session ID acquired from the login API to execute subsequent API calls, specifically for adding a role API.

### Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?gwsource=external
```

### Request Payload

```
{
"payload": {
 "name":"role_01",
 "description":"Adding a new role"
}
}
```

### Sample Response

```
{
"response": "Role added successfully",
"message": "Role added successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

## Reference

### Understanding the sample URL:

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

## Authentication Using a Service Account

For accessing APIs, you can login via two types of accounts:

- Service account

  A **Service account** represents a non-human entity such as an application or a service. It is used for automated processes or system-to-system interactions without human intervention.

  For accessing APIs with a service account, you need to get the Access Token by providing Client ID and Client Secret in get-service-token API. This Access Token can then be used for accessing other APIs.

  **Note:** Access Token Validity is 30 minutes by default and it can be configured in **Settings** > **Authentication** > **oAuth Settings**.

## Retrieve Access Token using get-service-token API

The API provides a streamlined process for retrieving service tokens related to account management tasks.

### Before you begin

• Make sure you have valid login credentials for accessing the system.

### Request Structure

| | |
|---|---|
| **Endpoint:** | `/acctmgmt-get-service-token` |
| **Type:** | `POST` |
| **Sample URL:** | `https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-get-service-token?gwsource=external`<br>To understand the elements of the sample URL, click here. |
| **Headers:** | |
| **Content-Type:** | application/json |
| **Authentication:** | Yes |
| **Request timeout period** | 15 minutes |

**Input Parameters**

| | Description |
|---|---|
| Authorization<br>*Header* | (Mandatory) Please form a string in this format <Client ID>:<Client Secret> and do base64 encoding. Then prepend a key 'Basic' before the encoded value. Final value should be "Basic <EncodedValue>".<br>**Type:** *String*<br>**Example:** "admin" |

**Input Parameters (continued)**

| | Description |
|---|---|
| Content-Type<br>*Header* | (Mandatory) The parameter should be set to `application/json` to specify the nature of the data in the payload.<br>**Type:** *String*<br>**Example:** "application/json" |
| grant_type<br>*Payload* | (Mandatory) Payload Type should be "Form". The value of the param should be "Client_Credentials".<br>**Type:** *Text* |

## Response Structure

- **Status Code:** 200 Ok
- **Message:** Successful
- **Headers:**
  - **Content-Type:** application/json

**Response Parameters**

| Name | Description |
|---|---|
| response | The response contains the attributes needed to retrieve the access token. |
| message | Success message or failure description in case of error. |
| appStatusCode | Application specific status code for the response. Will be non-null for failure response. |
| tags | More info in case of failure response. |

## Status Codes

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 200 OK | NA | Successful |

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 400 Bad request | ACCT_SA_003 | Service account is invalid/not found::[Service account not found in the database] |
| 400 Bad request | OAUTH_CLNT_015 | Client Password is incorrect::[Invalid Client credential] |
| 400 Bad request | ACCT_SA_001 | Invalid Request::[Invalid client Id or secret] |
| 500 Internal Server Error | avx-common-011 | Error while processing. |

## Sample Request/Response

### Use Case

Retrieve Access Token.

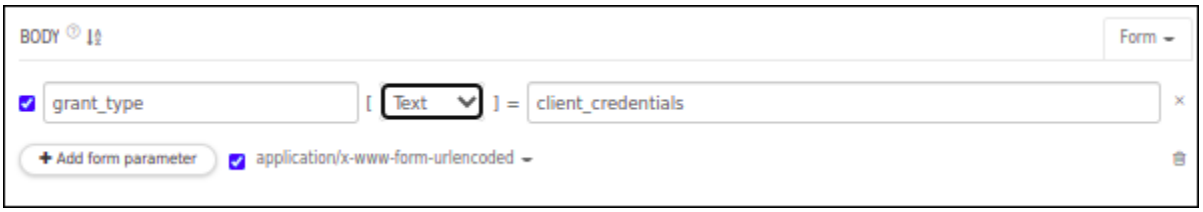
### Request URL

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-get-service-token?gwsource=external
```

**Content-Type:** application/x-www-form-urlencoded

**Authorization:** Basic
NTIxYzNhZDItZWE0ZS00NDdiLWE1MWItOTYyMWJiN2VhMTI2OjU1QVUjTk84JSpaaGd2TmZhWVVtdHZYMGRrRWhvZ

### Request Payload




### Sample Response

```
{
"response":
 "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBj
 NGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncmFudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqIDI7
 GYf4cWx6VwbjGD_0",
"message": null,
"appStatusCode": null,
"tags":{},
```

```
"headers": null
}
```

### What's Next

- **Using Access Token in the header for further API calls**

### Reference

**Understanding the sample URL:**

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

## Using Access Token in the header for further API calls

The access token retrieved using the get-service-token API can be used in the header for making further API calls.

**In this section, as an example, we are using the access token with the API call for adding a resource.**

## Before you begin

- Access Token is obtained from the get-service-token API.
- Ensure that the Access Token is valid and has not expired.

## Request Structure

| | |
|---|---|
| **Endpoint:** | /resource |
| **Type:** | POST |
| **Sample URL:** | https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external<br><br>To understand the elements of the sample URL, click here. |
| **Headers:** | |
| **Content-Type:** | application/json |

**Input Parameters**

| Name | Description |
|---|---|
| Token<br><br>*Header* | (Mandatory) Use token retrieved from login API.<br><br>**Type:** *String*<br><br>**Example:** eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBjNGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncmFudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqIDI7GYf4cWx 6VwbjGD_0 |
| gwsource<br><br>*Query* | (Mandatory) Source from which the request is triggered. The values can be:<br><br>• web<br>• external<br><br>**Type:** *String* |

**Input Parameters (continued)**

| Name | Description |
|---|---|
| Payload<br>*String* | (Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section. |

## Payload

| Name | Description |
|---|---|
| name<br>*String* | (Mandatory) Name of the resource to create. Name cannot be duplicated.<br>**Example:** "resource_1" |
| description<br>*String* | (Optional) Description of the resource.<br>**Example:** "This is a sample resource." |

## Response Structure

- **Status Code:** 201 Created
- **Message:** Resource added successfully
- **Headers:**
  - **Content-Type:** application/json

**Response Parameters**

| Name | Description |
|---|---|
| response | Contains the response attributes for resource added successfully. |
| message | Success message or failure description in case of error. |
| appStatusCode | Application specific status code for the response. Will be non-null for failure response. |
| tags | More info in case of failure response. |

## Status Codes

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 201 Created | null | Resource added successfully |

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 409 Conflict | RBAC_RE_005 | Resource with the given name already exists |
| 400 Bad Request | VALIDATION_ERROR_0004 | 'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty |
| 400 Bad Request | VALIDATION_ERROR_0004 | Invalid "name". |
| 401 Unauthorized | AVX_GW_012 | Unauthorized access, reason - Invalid Token |
| 407 Proxy Authentication Required | AVX_GW_011 | Session validation failed, reason - Session information is missing. |

## Sample Request/Response

### Use Case

Add a resource using API with Access Token.

### Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external
```

### Request Payload

```
{
 "payload": {
 "name": "resource_1",
 "description": "This is a sample resource."
 }
 }
```

### Sample Response

```
{
 "response": "Resource added successfully",
 "message": "Resource added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

### Reference

**Understanding the sample URL:**

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

## Fetch IP Footprints Across Sources

Fetches the list of sources where the IP traces are found. It is a solution for retrieving IP trace data from multiple sources through a unified, generic API.

### Before you begin

- Verify ACF permission for IP Search
  1. Go to **Platform > IDENTITY > Role**.
  2. Under **Role**, click the role name, select the **Authorized functions** tab.
  3. Expand **DDI+ > IP Compliance**.
  4. Select **IP Search** to ensure the permission is enabled.

## Request Structure

| | |
|---|---|
| **Endpoint:** | /ddi-ip-footprints |
| **Type:** | POST |
| **Sample URL:** | https://<IP/HostName/TenantName>:<GWPORT>/avxapi/ddi-ip-footprints?gwsource=external<br><br>To understand the elements of the sample URL, click here. |
| **Headers:** | |
| **Content-Type:** | application/json |

**Input Parameter**

| Name | Description |
|---|---|
| sessionId<br><br>*Header* | (Mandatory) After successfully logging in, a unique identifier assigned to a user's session after successful authentication. The session ID remains valid until it expires. The session ID is a string value.<br><br>**Example:** "ce7f1a14-2bf9-4e4a-89a8-bc780a255813" |
| Or | |
| username<br><br>*Header* | (Mandatory) AppViewX login username, represented as a string value.<br><br>**Example:** "User" |
| password<br><br>*Header* | (Mandatory) AppViewX login username, represented as a string value.<br><br>**Example:** "AppViewX@123" |
| Payload | (Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section. |

## Payload

| Name | Description |
|---|---|
| ipAddress<br><br>*String* | (Mandatory) Enter the IP address to retrieve the list of sources containing its trace details.<br><br>**Example:** 10.10.10.3 |

## Response Structure

- **Status Code:** 200 OK
- **Message:**
- **Headers:**
  - **Content-Type:** application/json

**Response Parameters**

| Name | Description |
|---|---|
| response | Contains the response attributes for the get policy request. |
| message | Success message or failure description in case of error. |
| appStatusCode | Application specific status code for the response. Will be non-null for failure response. |
| tags | More info in case of failure response. |

## Status Codes

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 200 OK | | |
| 400 Bad Request | VALIDATION_ERROR_0004 | Invalid 'ipAddress' |
| 400 Bad Request | VALIDATION_ERROR_0004 | Mandatory Field 'ipAddress' is missing or empty |

## Sample Request/Response

**Use Case**

This API is designed to retrieve a list of data sources that contain traces for a given IP address.

**Request URL**

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/ddi-ip-footprints?gwsource=external
```

**Request Payload**

```
{
  "payload": {
    "ipAddress": "10.10.10.3"
```

```
 }
}
```

**Sample Response**

```
{
 "sources": ["adc", "cmdb", "tanium", "forwardNetworks"]
}
```

## What's Next

- **Fetch IP Trace Details by Source**

## Reference

**Understanding the sample URL:**

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

# Fetch IP Trace Details by Source

This API takes a source name and an IP address as input parameters. It queries the specified source to retrieve detailed trace information related to the given IP address. The response may include additional data from associated sub-sources, providing a comprehensive view of the IP trace.

## Before you begin

- Verify ACF permission for IP Search
  1. Go to **Platform > IDENTITY > Role**.
  2. Under **Role**, click the role name, select the **Authorized functions** tab.
  3. Expand **DDI+ > IP Compliance**.
  4. Select **IP Search** to ensure the permission is enabled.
- Verify that the entered IP address is valid.
- Confirm that the specified source name is accurate and recognized by the system.

## Request Structure

| | |
|---|---|
| **Endpoint:** | `/ddi-ip-trace-details-by-source` |
| **Type:** | `POST` |
| **Sample URL:** | `https://<IP/HostName/TenantName>:<GWPORT>/avxapi/ddi-ip-trace-details-by-source?gwsource=external`<br><br>To understand the elements of the sample URL, click here. |
| **Headers:** | |
| **Content-Type:** | application/json |

**Input Parameter**

| Name | Description |
|---|---|
| sessionId<br><br>*Header* | (Mandatory) After successfully logging in, a unique identifier assigned to a user's session after successful authentication. The session ID remains valid until it expires. The session ID is a string value.<br><br>**Example:** "ce7f1a14-2bf9-4e4a-89a8-bc780a255813" |
| Or | |
| username | (Mandatory) AppViewX login username, represented as a string value. |

**Input Parameter (continued)**

| Name | Description |
|---|---|
| *Header* | **Example:** "User" |
| password | (Mandatory) AppViewX login username, represented as a string value. |
| *Header* | **Example:** "AppViewX@123" |
| Payload | (Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section. |

## Payload

| Name | Description |
|---|---|
| source | (Mandatory) Enter the source of the IP address. |
| *String* | **Example:** cmdb |
| ipAddress | (Mandatory) Enter the IP address to retrieve the list of sources containing its trace details. |
| *String* | **Example:** 10.10.10.3 |

## Response Structure

- **Status Code:** 200 OK
- **Message:**
- **Headers:**
  - **Content-Type:** application/json

**Response Parameters**

| Name | Description |
|---|---|
| response | Contains the response attributes for the get policy request. |
| message | Success message or failure description in case of error. |
| appStatusCode | Application specific status code for the response. Will be non-null for failure response. |

**Response Parameters (continued)**

| Name | Description |
|---|---|
| tags | More info in case of failure response. |

## Status Codes

| HTTP Code | appStatusCode | Response Message |
|---|---|---|
| 200 OK | | |
| 400 Bad Request | VALIDATION_ERROR_0004 | Invalid 'ipAddress' |
| 400 Bad Request | VALIDATION_ERROR_0004 | Mandatory Field 'ipAddress' is missing or empty |
| 400 Bad Request | VALIDATION_ERROR_0004 | Mandatory Field 'source' is missing or empty |
| 400 Bad Request | DNS_RECORDMGMT_026 | Invalid source. Requested source not supported for ip search |

## Sample Request/Response

### Use Case

This API is designed to retrieve detailed IP trace information from a specified source identified by source discovery.

### Request URL

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/ddi-ip-trace-details-by-source?gwsource=external
```

### Request Payload

```
{
  "payload": {
    "source": "cmdb",
    "ipAddress": "10.10.10.3"
  }
}
```

**Sample Response Example 1 (Single Source):**

```
{
  "response": {
    "DNS Details": [
      {
        "Record Type": "HOST_IPV4ADDR",
        "Vendor": "Infoblox",
        "type": "General",
        "Vendor Account Name": "infobloxSmall",
        "Domain Name": "test3",
        "Name": "test3"
      }
    ]
  }
}
```


### Sample Response Example 2 (Multiple Sub-Sources)


```
{
  "cmdb_source_1": [
    {
      // IP trace details for CMDB sub-source 1
    }
  ],
  "cmdb_source_2": [
    {
      // IP trace details for CMDB sub-source 2
    }
  ]
}
```


## What's Next

- **Fetch IP Footprints Across Sources**

## Reference

### Understanding the sample URL:

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.