IP Address Manager

User Guide v4.0.0

Notices

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE. BY CLICKING ON THE "I ACCEPT THE TERMS OF THE LICENSE AGREEMENT" BUTTON, OPENING THE PACKAGE, DOWNLOADING THE PRODUCT, OR USING THIS PRODUCT, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "I DO NOT ACCEPT THE TERMS OF THE LICENSE AGREEMENT" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND, OR DO NOT DOWNLOAD THE PRODUCT. YOUR GENERAL TERMS OF BUSINESS DO NOT APPLY.

General

In this software license agreement:

a) "Mindarray" means Mindarray Systems Pvt Ltd., 14/3, Magnet Corporate Park. 100 Feet Road, S.G Highway, Near Sola Bridge Opp. Grand Cambay, Thaltej, Ahmedabad, Gujarat. India.

b) "Customer" means the individual(s), organization or business entity buying a license of the software from Mindarray or its distributors or its resellers.

c) "Software" means computer programs (and their storage medium) supplied by Mindarray and known collectively as "Mindarray IP Address Manager" in which Mindarray has propriety rights for its any user manuals, example code, operating instructions, brochures and all other documentation relating to the said computer programs (the expression "software" to include all or any part or any combination of software).

License Grant

This license grants you the following rights:

a) Software product: Mindarray grants you an exclusive license to use the software for the sole purposes of designing, developing, and testing your software components or applications ("applications"). You may install the software on any computer in your organization.

b) Electronic documents: Solely with respect to electronic documents included with the software, you may make an unlimited number of copies (either in hardcopy or electronic form), provided that such copies shall be used only for internal purposes and are not republished or distributed to any third party.

c) License file: A file provided at the time of sale uniquely identifies each license. This license grant is contingent upon the purchase of a license file from Mindarray or one of Mindarray's resellers.

d) Sample code: Mindarray grants you the right to use and modify the source code parts of the software that are listed in the "projects" and "scripts" subdirectories (if available).

e) Redistribution: The software is made available for download solely for use by end users according to the license agreement. Any reproduction or redistribution of the software not in accordance with the license agreement is expressly prohibited.

f) Trial software: If the software is installed without a serial number then, notwithstanding other sections of this license, you may use the software for up to 30 days after installation.

g) Not for resale software: If the software is labeled as "not for resale " or "NFR" then, notwithstanding other sections of this license, you may not resell, or otherwise transfer the value of software, neither distribute any redistributables.

h) Reservation of rights: Mindarray reserves all rights not expressly granted to you in this license agreement. The license is granted to the customer on a non-exclusive-basis which means that Mindarray will grant the license also to their individuals, organizations and business entities.

i) This license agreement consists of no obligations for Mindarray to offer support (services), help (services) or maintenance (services) relating to the software. Obligations for Mindarray to offer maintenance (services) relating to the software can only arise from a maintenance agreement between Mindarray and customer. General terms of business of the customer do not apply.

Upgrades and Supplements

If the software is labeled as an upgrade, you must be properly licensed to use a product identified by Mindarray as being eligible for the upgrade in order to use the software. Software labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this license unless we provide other terms along with the update or supplement. If the software is an upgrade of a component or a package or software programs that you licensed as a single product, the software may be used and transferred only as part of that single product package.

Limitation on Reverse Engineering, Decompilation, And Disassembly

Customer may not reverse engineer, decompile, or disassemble the software, except and only to the extent that it is expressly permitted by applicable law notwithstanding this limitation.

Termination

Without prejudice to any other rights, Mindarray may cancel or dissolve this license agreement if the customer does not abide by the terms and conditions of this license agreement, in which case customer must destroy all copies of the software and all of its component parts.

Limited Warranty

Mindarray warrants that for a period of ninety (90) days from the date of shipment from Mindarray. The media on which the software is furnished will be free of defects in materials and workmanship under normal use.

The software substantially conforms to its published specifications. Except for the foregoing, the software is provided as is. This limited warranty extends only to the customer as the original licensee. Customer's exclusive remedy and the entire liability of Mindarray and its suppliers under this limited warranty will be, at Mindarray or its service center's option, repair, replacement, or refund of the software if reported (or, upon request, returned) to the party supplying the software to the customer. In no event does Mindarray warrants that the software is error-free or that customer will be able to operate the software without problems or interruptions. The customer will safeguard Mindarray against any claim relating to the use of the software by the customer. This warranty does not apply if the software: (a) has been altered, except by Mindarray; (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Mindarray; (c) has been subjected to abnormal physical or electrical stress misuse, negligence, or accident; (d) is used in high-risk activities, including the operation of nuclear facilities, aircraft navigation, air traffic control, weapons systems, life support or medical applications for use in any circumstance in which the failure of the software could lead directly to death, personal injury or damage to properties or the environment.

Limitation of Liability and Remedies

NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR MULTIPLE DAMAGES SUCH AS BUT NOT LIMITED TO, LOST BUSINESS OR PROFITS, LOSS OF GOODWILL, WORKS TOP PAGE AND DATA LOSS), THE ENTIRE LIABILITY OF MINDARRAY AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS LICENSE AGREEMENT AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING (EXCEPT FOR ANY REMEDY OF REPAIR OR REPLACEMENT ELECTED BY MINDARRAY WITH RESPECT TO ANY BREACH OF THE LIMITED WARRANTY) SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE. MINDARRAY IS RELIEVED OF ANY OBLIGATION TO PAY DAMAGES IF THE CUSTOMER HAS NOT UPGRADED THE SOFTWARE WHEN POSSIBLE. THE FOREGOING LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS (INCLUDING SECTIONS 4, 5 AND 6 ABOVE) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

Entire Agreement

This license agreement (including any addendum or amendment to this license agreement which is included with the software) is the entire agreement between you and Mindarray relating to the software and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with

respect to the software or any other subject matter covered by this license agreement. To the extent the terms of any Mindarray policies or programs for support services conflict with the terms of this license agreement, the terms of this license agreement shall control.

The customer is not allowed to alienate or transfer any rights relating to this license agreement without the written approval of Mindarray.

THIS AGREEMENT SHALL BE CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE INDIAN GOVERNMENT AND THE INDIAN COURTS SHALL HAVE SOLE JURISDICTION IN ANY DISPUTE RELATING TO THESE CONDITIONS. ALL DISPUTES HEREUNDER SHALL BE RESOLVED EXCLUSIVELY IN THE APPROPRIATE COURT IN THE CITY OF AHMEDABAD, INDIA. If any part of these conditions shall be or become invalid or unenforceable in any way and to any extent by any existing or future rule of law, order, statute or regulation applicable thereto, then the other conditions shall remain in full force and effect as all other provisions.

The conditions of this license agreement remain applicable after the termination of this license agreement if this results from the nature of the condition.

Copyright

The software is protected by copyright and other intellectual property laws and treaties. Mindarray or its suppliers own the title, copyright, and other intellectual property rights in the software. The granting of a license does not constitute a transfer of any intellectual property right. The software is licensed, not sold.

Contents

1. Introduction

Motadata IP Address Manager is a user-friendly tool that provides detailed visibility into the IP addresses, DHCP scope, and subnet use. Use IP Address Management (IPAM) to plan the network growth, view available and used IP address spaces, and troubleshoot IP address conflicts. IP Address Manager also allows you to manage the Windows and Cisco DHCP servers.

1.1. Features of the Motadata IP Address Manager

- IP Address tracking and actual information
- Automatically get the current status of each IP Address
- Get IP Address details with IP Address utilization
- Subnet address utilization details
- End-to-end IP History and audit
- Role-based administration (Admin and User)
- Easy to add subnets, supernets, and Gateways
- DHCP server support
- Flexibility for scanning subnets
- Global search to get details of IP Address
- Configuring alerts
- Report functionality with export and schedule feature
- API Support
- Supports Windows platform
- Rogue Detection
- IP Requests

2. Access IP Address Manager

Fig 1: IPAM Login Screen

Enter your username and password to sign in to your account.

- **Default Username**: admin
- **Default Password**: admin

2.1. Forgot Password

If you don't remember your password, use the "Forgot Password" feature to reset your password.

1. Click on Forgot Password?.
2. Provide the username, and a verification code will be sent to the email ID associated with the username.
3. Insert the verification code you receive in the email and generate a new password again.
4. Type the new password and click '**Update**'.

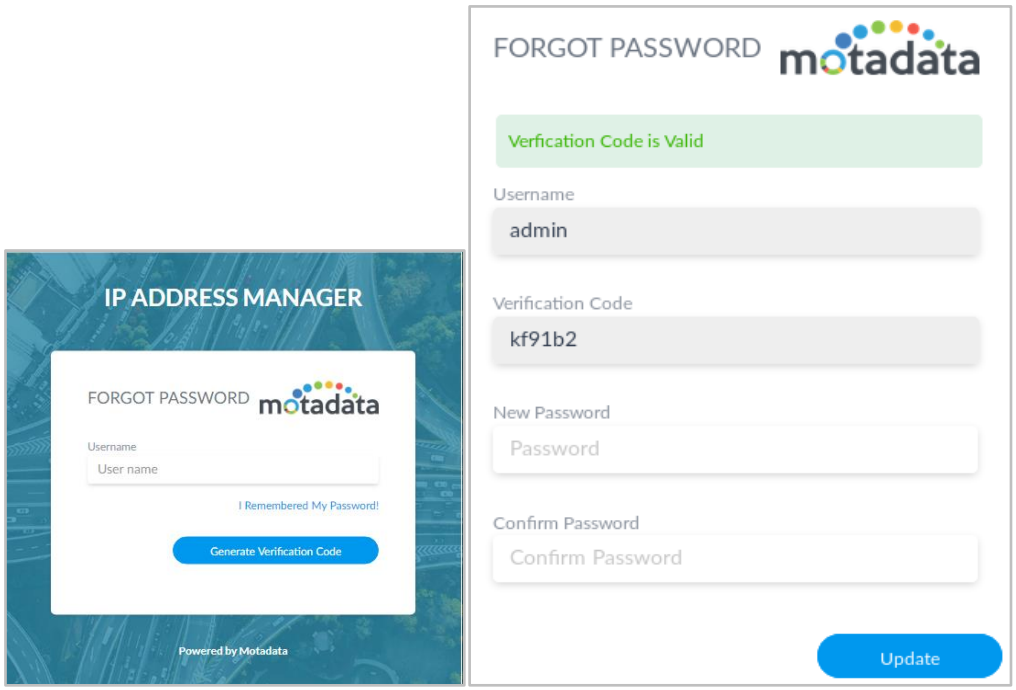


Fig 2: Forgot Password Screen (left) Provide username (right), insert verification code, and create a new password

Note: The generated verification code will be valid for 15 minutes.

IPAM will redirect you to the homepage upon login.

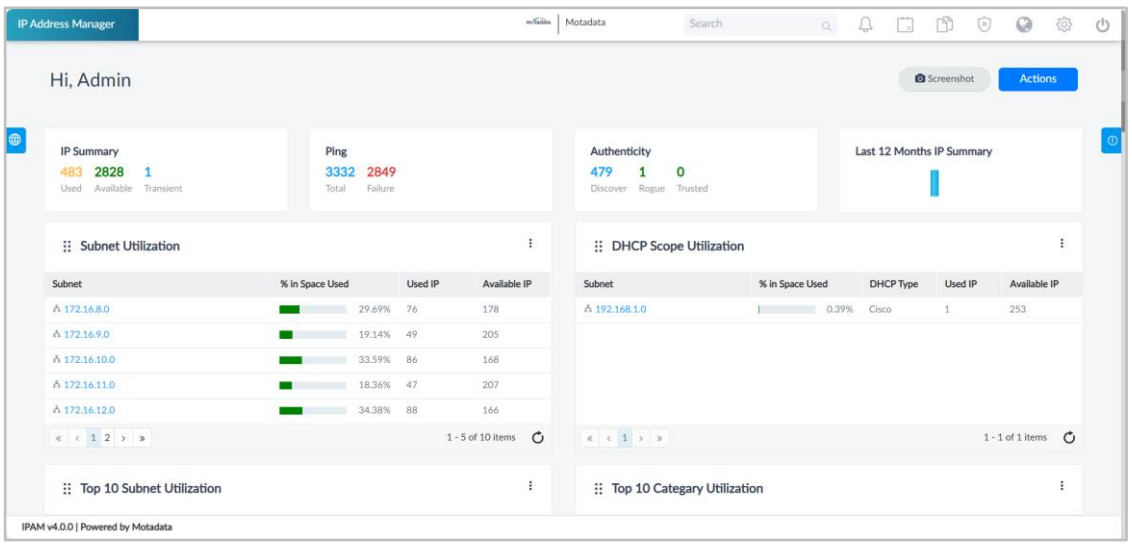


Fig 3: IPAM Home Page

3. Home Page

Homepage or the Dashboard provides a summary of all the activities happening in IP Address Manager. The page provides links to add, view, and manage Subnets and Supernets quickly. The homepage consists of:

- Capture Screenshot
- Actions
- IP Usage Summary
- Ping Count
- Authenticity Count
- Last 12 Months IP Summary
- Subnet Utilization
- DHCP Scope Utilization
- Top 10 Subnet Utilization
- Top 10 Category Utilization
- IP Availability Summary
- DNS Status Summary
- Top 10 Vendor Summary
- Conflict IP Summary
- Recently Discovered MAC
- IP Events | Top 25

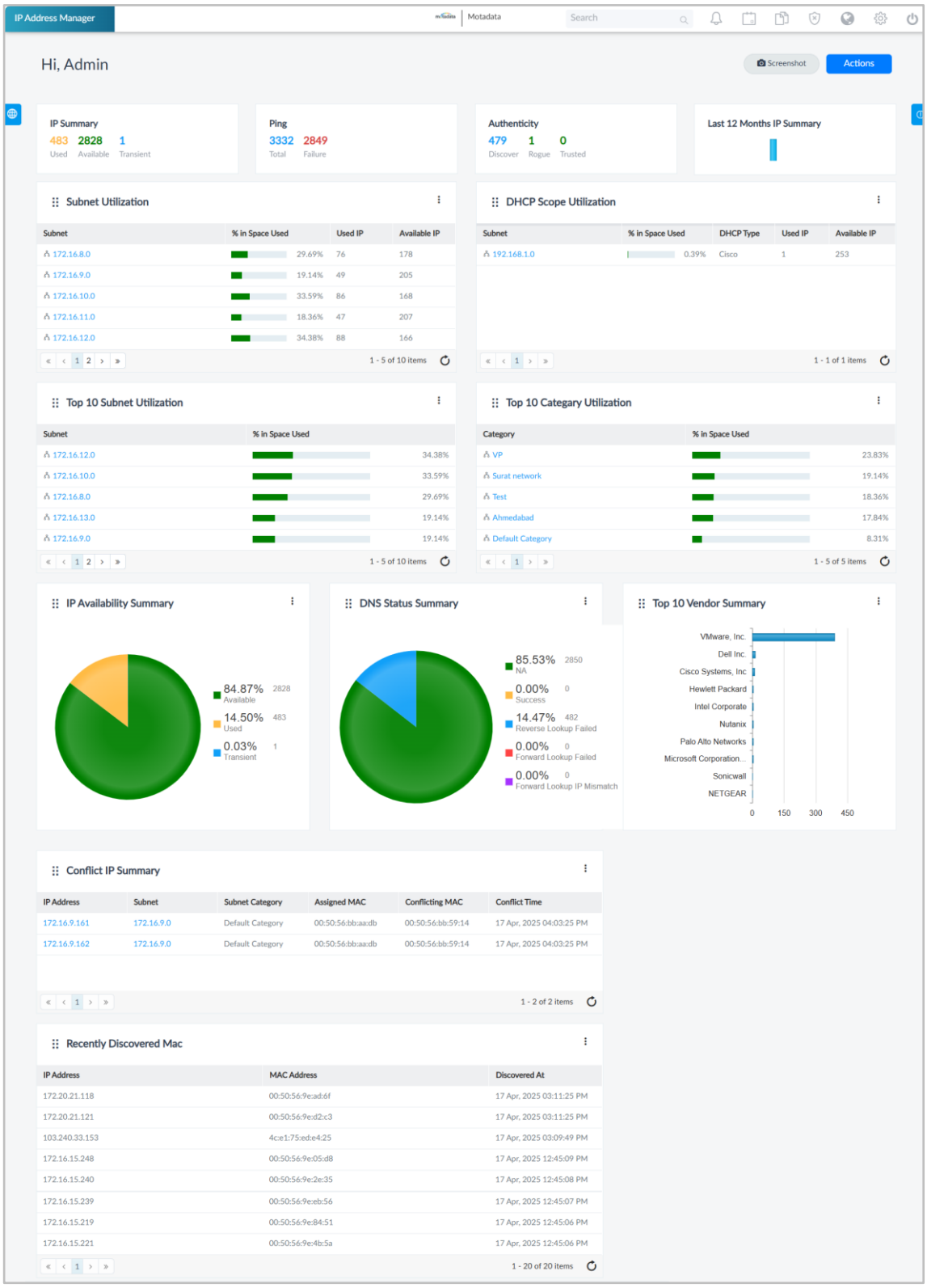


Fig 4: Home Page

3.1. System bar

Fig 5: System bar

From left to right, the system bar includes the following components:

- Home
- Logo and Product name
- Search bar: for global search
- Alerts
- Event Notifications
- Reports
- Rogue Detection
- IP Requests
- Settings
- Logout

3.2. Actions

IP Address Manager allows you to quickly add subnets and supernets directly from the home page using the **Actions** button, making it easy to start building and organizing your IP address space.

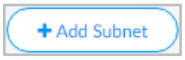
IP Address Manager mainly works on a subnet address. It supports both IPv4 and IPv6 addresses. So below are the options available for adding a subnet and supernet address.

- **Subnet**: When users do not have any DHCP server, they can add a new subnet manually or through a CSV file.
- **DHCP Server**: The user can easily add a DHCP server and automatically maintain all subnet addresses and IP Address details.

Add Subnet

You can add subnets from multiple locations:

- Actions
- Inventory
- Discovery Settings

You can add an IPv4 or IPv6 subnet by clicking on the 

button from the top or from the left panel of Inventory's  button. You can add a subnet manually or by importing a CSV file.

- **Add Subnet manually**: Manually add the subnet when there are only a few subnet addresses.
- **Import from CSV**: Import the CSV file when adding multiple subnet addresses in a single go.

i. Add IPv4 Subnet Manually

You can add a subnet manually by inserting its details. Below are the available fields with their descriptions:

- **Local Subnet**: Select this option if your local network's IP/Devices need to be discovered using IPAM.
- **Remote Subnet**: Select this option if any other network's IP/devices need to be discovered using IPAM. Once you select the Remote Subnet, an option to input the Gateway IP opens up. You can use another network's Gateway IP to establish the connection between the Local and Remote via Gateway IP. Here, SNMP Community is a user-specific field.
  Note: Remote Subnet supports only IPv4 addresses.

- **Select Category**: By default, the category is a Default category. You can create a custom category using the '+Add Category' 

button. The category is simply the logical classification to group the subnet in IPAM.

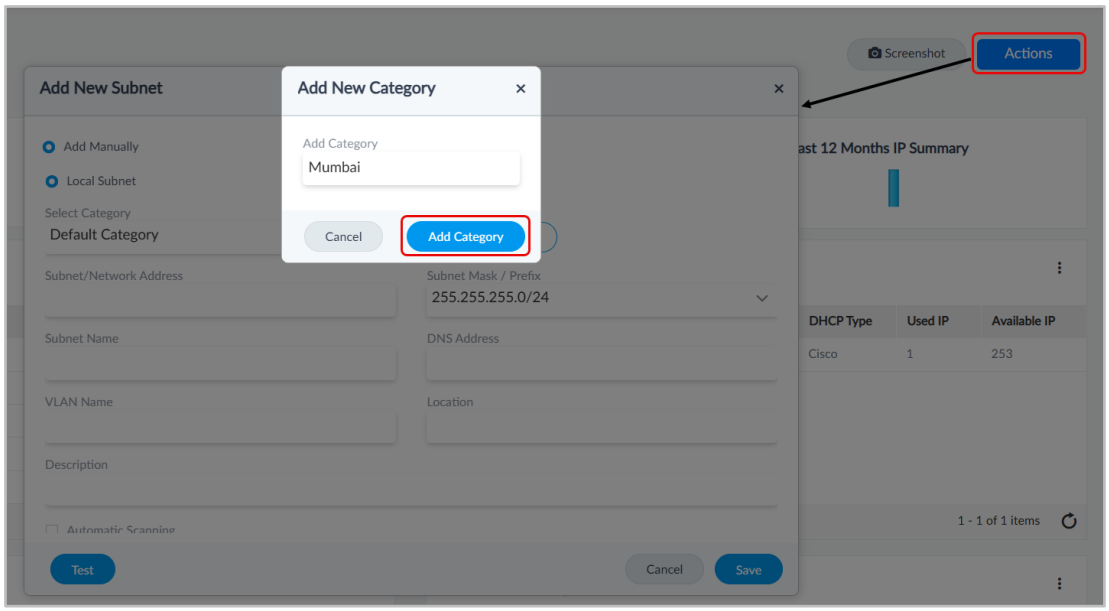


Fig 6: Add New Category

- **Subnet/Network Address**: Enter a valid Subnet/Network Address. (**e.g.** 192.168.0.0)
- **Subnet Mask/Prefix**: Select an appropriate Subnet Mask from the dropdown. The subnet mask defines a range of IP addresses in the network. Use this dropdown to select your subnet mask. By default, the subnet mask is set with

255.255.255.0/24. You can select the subnet mask from the list of 16 CIDR to 31 CIDR.

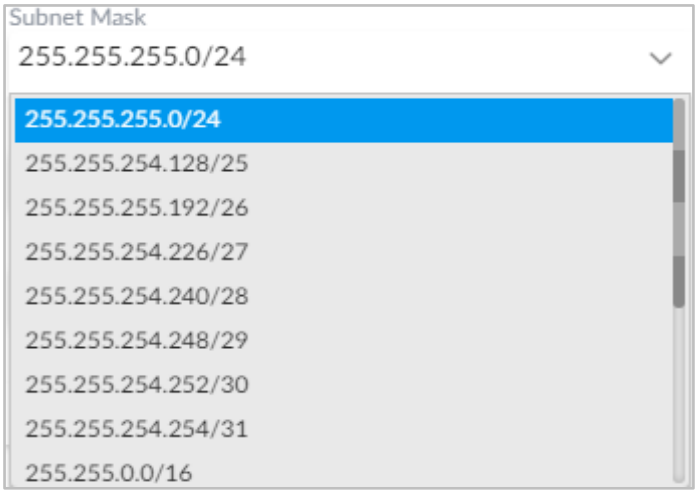


Fig 7: Subnet Mask List

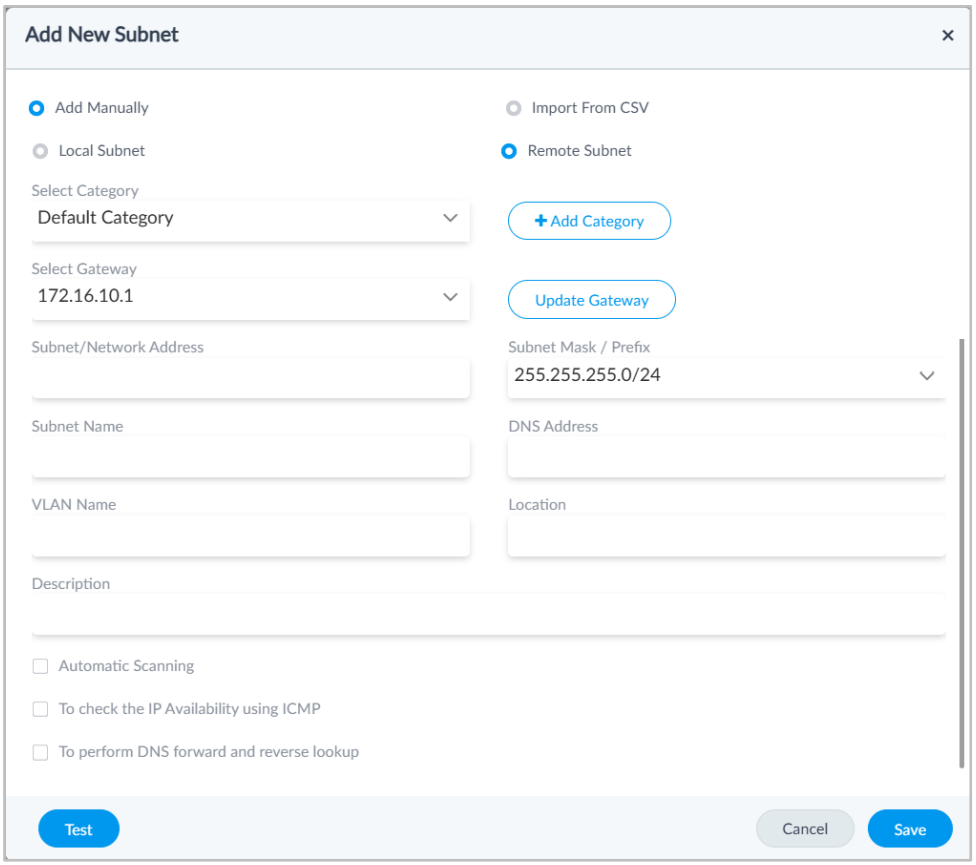


Fig 8: Add New Subnet

- **Subnet Name**: The System automatically copies the Subnet/Network Address as the Subnet Name. You can replace the Subnet address by adding your desired value here.
- **DNS Address**: Enter a valid **DNS Address** of your network (e.g., 255.255.255.255)
- **VLAN Name**: Enter Subnet and VLAN name (e.g. V12345)
- **Location**: Enter the Location details of the subnet address. (e.g. Server Room 1)
- **Description**: Enter the Description for the subnet address. (e.g. Home Network)

- **Automatic Scanning**: You can enable the 'Automatic Scanning' or manually scan the Subnet later. For automatic scanning, check 

true.
- Select the timeframe (Day/Week/Month) and the value. The system will run a thread to scan the Subnets automatically on a given period.
- **Check Availability using ICMP**: To check the availability of IP Addresses using ping, check 

true.
- **Forward and Reverse Lookup**: To get the information for the forward and reverse DNS lookup, check 

true. (Prerequisite: Point 10 is mandatory)

Once all the fields are configured, **test** the validity of your Subnet IP and DNS address. If the test is successful, the system will display a green prompt.

Next, Save the configuration.

ii. Add IPv6 Subnet Manually

You can add an IPv6 subnet manually by filling in the below details:

- **Local Subnet**: Select this option if your local network's IP/Devices need to be discovered using IPAM.

  Note: **Remote Subnet supports only IPv4 addresses.**

- **Select Category**: By default, the category is a Default category. You can create a custom category using the '+Add Category' 

button. The category is simply a logical classification to group the subnet in IPAM.
- **Subnet/Network Address**: Enter a valid Subnet/Network Address. (e.g. ff05::)
- **Subnet Mask**: Select an appropriate Subnet Mask from the dropdown. The subnet mask defines a range of IP addresses in the network. Use this dropdown to select your subnet mask. By default, the subnet mask for IPv6 is set to **128**. You can select the subnet mask from the 1 to 128 prefix list.

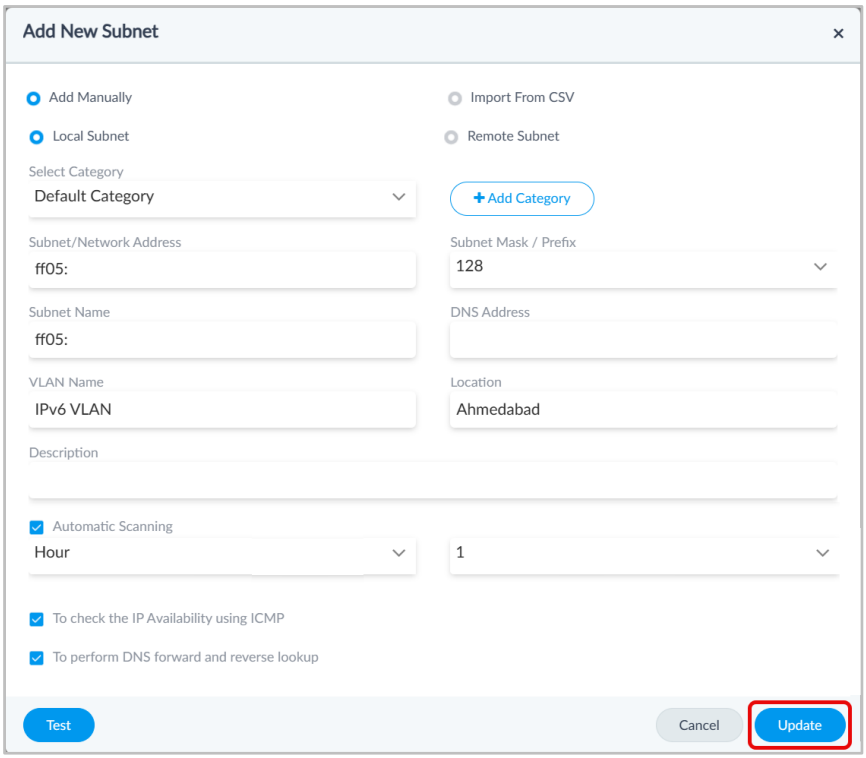
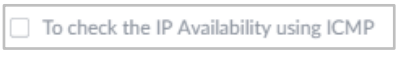


Fig 9: Add New Subnet

- **Subnet Name**: The system automatically copies the Subnet/Network Address as the Subnet Name. You can replace the Subnet address by adding your desired value here.
- **DNS Address**: Enter the DNS Address.
- **VLAN Name**: Enter Subnet and VLAN name (e.g. IPv6 VLAN)
- **Location**: Enter the location details of the subnet address. (e.g. Server Room 1)
- **Description**: Enter the description for the subnet address. (e.g. Home Network)
- **Automatic Scanning**: You can enable the 'Automatic Scanning' or manually scan the Subnet later. For automatic scanning, check  true.

- Select the timeframe (Hour/Day/Month) and the value. The system will run a thread to scan the Subnets automatically on the given period.
- **Check Availability using ICMP**: To check the availability of IP Addresses using ping, check  true.

- **Forward and Reverse Lookup**: To get the information for the forward and reverse DNS lookup, check  true. (Prerequisite: Point 10 is mandatory)

- Once all the fields are configured, **test** the validity of your Subnet IP and DNS address. If the test is successful, the system will display a green prompt.
- **Next,** Save the configuration.

iii. Import Subnets from CSV

You can also add a subnet by importing a CSV file using 'Import from CSV'. Download the sample file using the **Download Sample CSV** option. Enter data as per the sample file, upload the file, and click on the Import button.

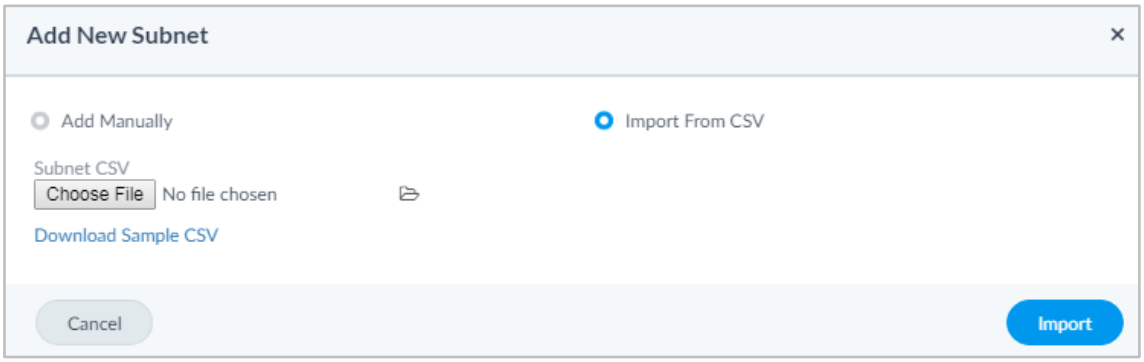


Fig 10: Add a New Subnet by importing a file from CSV

Add Supernet

A supernet is a large network combining smaller subnets into a single, broader address range. This process is called supernetting or route aggregation, and it's commonly used to simplify IP address management and reduce routing table entries.

Key Points About a Supernet:

- **Larger Range**: A supernet uses a shorter subnet mask covering more IP addresses than a typical subnet.
- **Combines Subnets**: It groups multiple contiguous subnets into one network block.

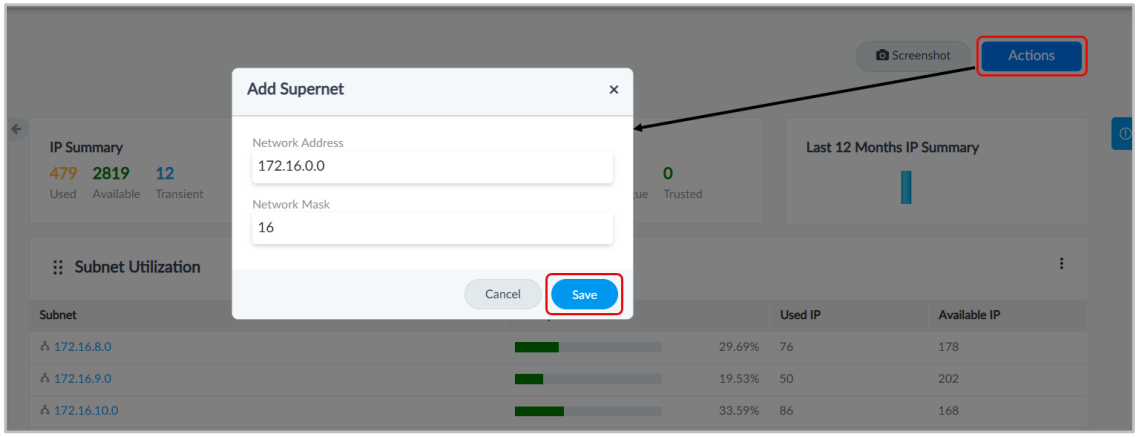


Fig 11: Add Supernet

Example:

If you have the following subnets:

- 192.168.1.0/24

- 192.168.2.0/24
- 192.168.3.0/24
- 192.168.4.0/24

You could combine them into a single supernet:

Supernet: 192.168.0.0/16

Network Mask: 255.255.0.0

This would cover IPs from 192.168.0.0 to 192.168.3.255.

Once added, the Supernet will appear in the Inventory as shown below.

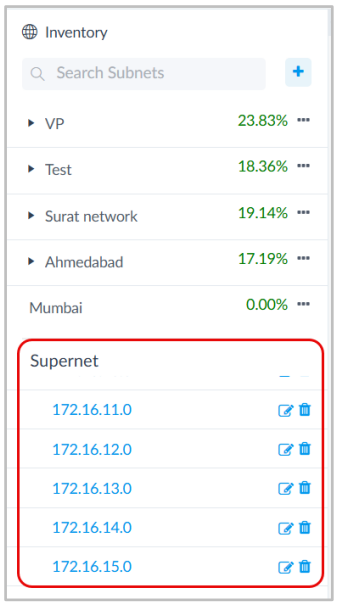


Fig 12: Supernet

3.3. Inventory (Left Panel)

To view the Inventory panel, click on the Globe  . The panel will open from the left side, as shown below.

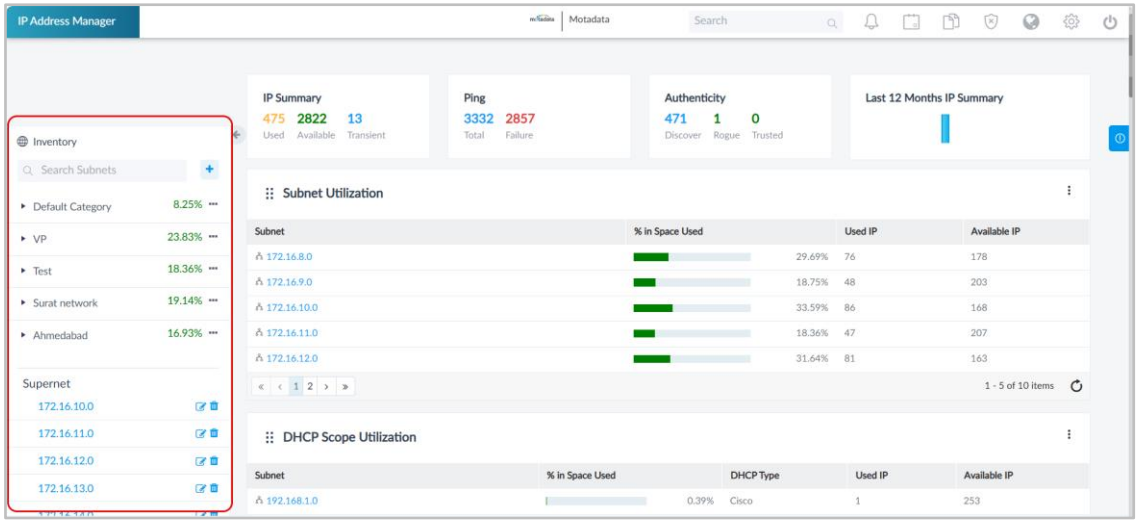


Fig 13: Inventory on Home Page

Here, you can perform the following operations:

Action Screen	Action Type	Action Description
+	Add Subnet	You can add a new subnet.
	Edit	You can edit a particular subnet.
	Delete	You can delete a particular subnet.
...	Actions	You can rename or delete a particular category. Also, you can delete a supernet.

At Inventory, you can view 3 sections:

- **Default Category**: Displays the details of the Subnet address with a particular category. You can move subnet addresses from one category to another by editing the subnet or by drag and drop. Also, you can add a new subnet by clicking on the + button.

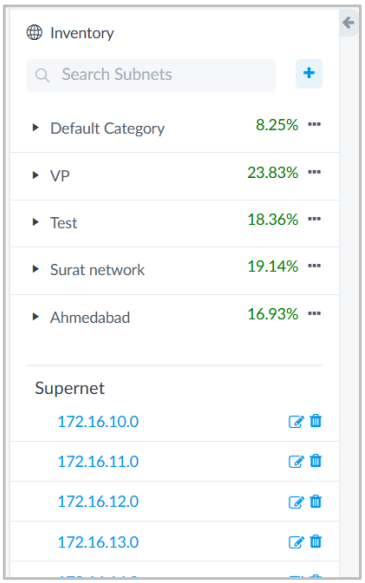


Fig 14: Inventory Panel

- **Search**: Enables searching for subnets in the inventory search bar. You can Edit and Delete the subnet address categories.

- **Supernet**: Displays the subnets belonging to a supernet address.

3.4. IP Events | Top 25 (Right Panel)

To view the IP Events, click the **Event Logs** button. The panel displays the list of the most recent 25 events. The events are arranged chronologically (most recent at the top).

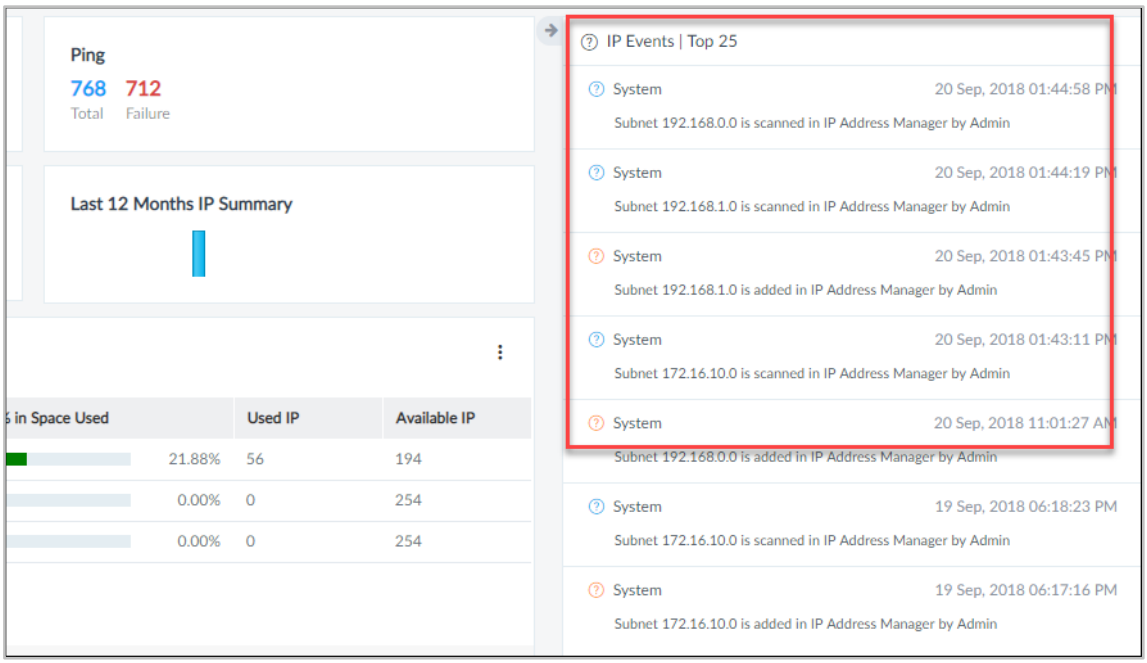


Fig 15: IP Events Menu on Home Page

The color of the icon indicates the type of event that occurred:

- **Orange**: A subnet or user is added to and deleted from the system.
- **Blue**: A subnet is scanned.
- **Red**: A conflict between IP addresses is recorded.

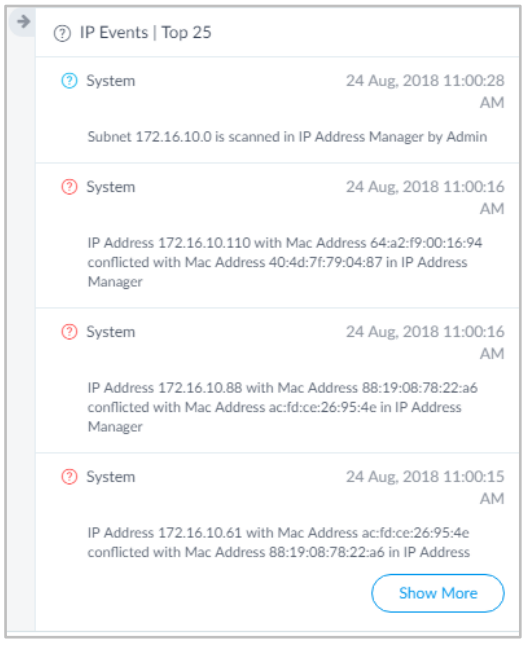


Fig 16: IP Events (Top 25)

Here, you can get details like conflict IP details, operations done by the user with the username, subnet scan information, and subnet add-delete operations with the username.

3.5. IP Summary

In IP Summary, you can get the exact count of Used, Available and Transient states IP Address.

- **Used**: The number of IP addresses currently in use.
- **Available**: The number of IP addresses available for use.
- **Transient**: The IP Address manager checks an IP address's current and previous status. If the current status is 'free' and the previous status is 'used', IP Address Manager keeps the address in the Transient state. Once the address is in a transient state, IPAM keeps it in the same status for the next 7 days before considering it as 'Available' (unless IP is used again).

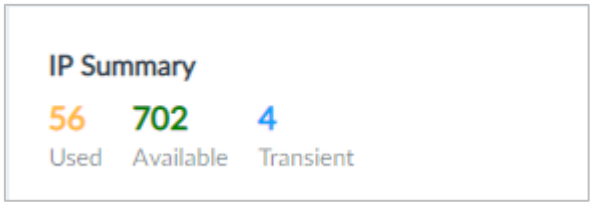


Fig 17: IP Summary

3.6. Ping

You can get the exact count of total and failed IP addresses in Ping. The total count shows the number of IP Addresses pinged by the IP Address Manager. Failure shows the number of IP addresses that didn't respond to the ping.

Note: The IP Address Manager application uses ICMP to ping the IP address. Enable the "To Check the IP Availability using ICMP" checkbox to view the Ping count while creating the Subnet, as shown below.

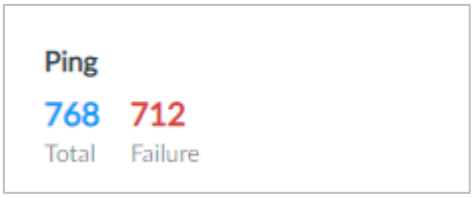


Fig 18: Ping

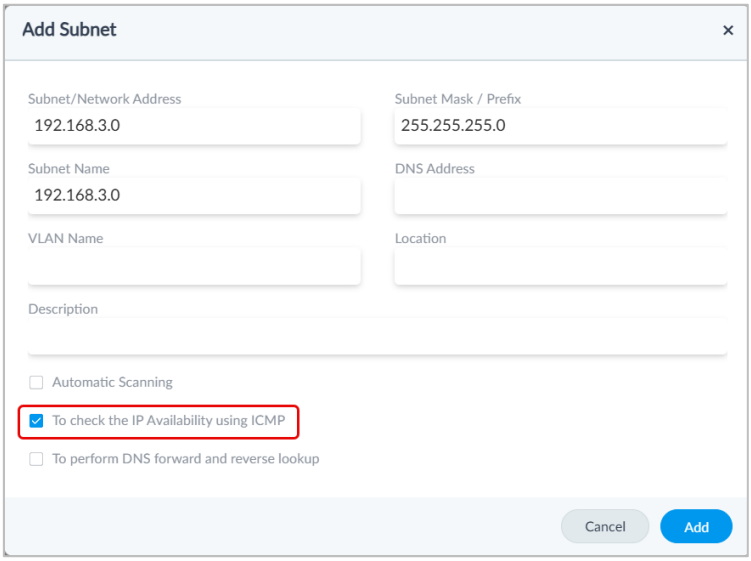


Fig 19: Enable "To Check the IP Availability using ICMP" option

3.7. Authenticity

Authenticity KPI displays the number of devices discovered, rogue, and trusted.

- **Discover** the total number of IP addresses used in the system. They can be marked as Rogue or Trusted.
- **Rogue**: Total IP addresses marked with the Rogue status.
- **Trusted**: Total IP addresses marked with the Trusted status.

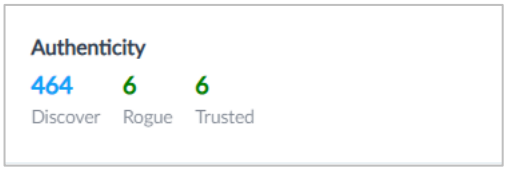


Fig 20: Authenticity

3.8. Last 12 Months IP Summary

The vertical bars in the graph (max 12) represent the year's months. The color of the vertical bars indicates the type of activity majorly performed that month. You can hover over the vertical bar to see the activity count. The vertical bars are displayed in 3 colors:

Orange: The bar is orange in color when

- A new subnet or DHCP has been added to IPAM.
- A Subnet or DHCP is deleted from IPAM.
- An IP address is marked as rogue or trusted.

Blue: The bar is in blue when

- A user is added or removed from IPAM.
- A subnet or DHCP is scanned in IPAM (manual or scheduled).

Red: The bar is in red when

- IP addresses conflict in IPAM.
- Subnet utilization goes above 80%.

Fig 21: Last 12 Month IP Summary

3.9. Subnet Utilization

Subnet utilization displays the list of all subnets present in IPAM. The widget displays:

- **Name**: Name of the subnet.
- **% in space used**: Percentage of IP addresses in use.
- **Used IP**: Count of used IP addresses.
- **Available IP**: Count of available IP addresses.

You can click the **More Options** ⋮ icon to export the details in PDF format.

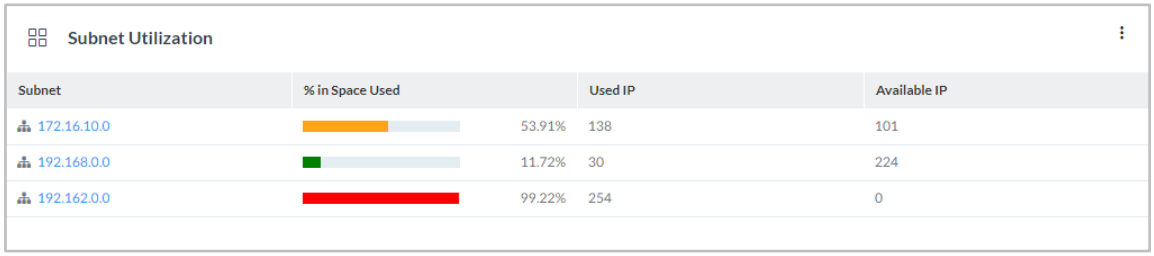


Fig 22: Subnet Utilization Details

Click on the name of a Subnet to get its details page. The details of a subnet are discussed in **Detailed Subnet** Summary (section 4).

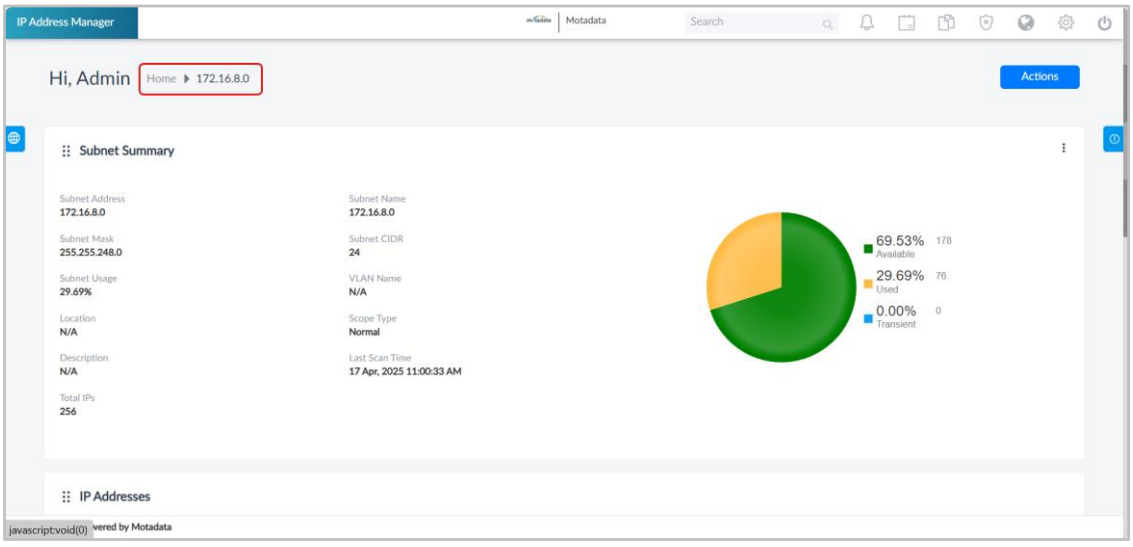


Fig 23: Details Subnet Summary

3.10. DHCP Scope Utilization

The widget displays the list of all subnets added as a DHCP server. The widget displays:

- **Name**: Name of the subnet.
- **% in space used**: Percentage of IP addresses in use.
- **DHCP Type**: DHCP server is added for Windows machines or Cisco machines.
- **Used IP**: Count of used IP addresses.
- **Available IP**: Count of available IP addresses.

It shows all subnet details of Windows and Cisco DHCP servers as subnets used in %, DHCP Type, Used IP, and Available IP. For more details about DHCP, refer to the DHCP Management section.

Also, you can click the **More Options** icon to export the details in PDF format.

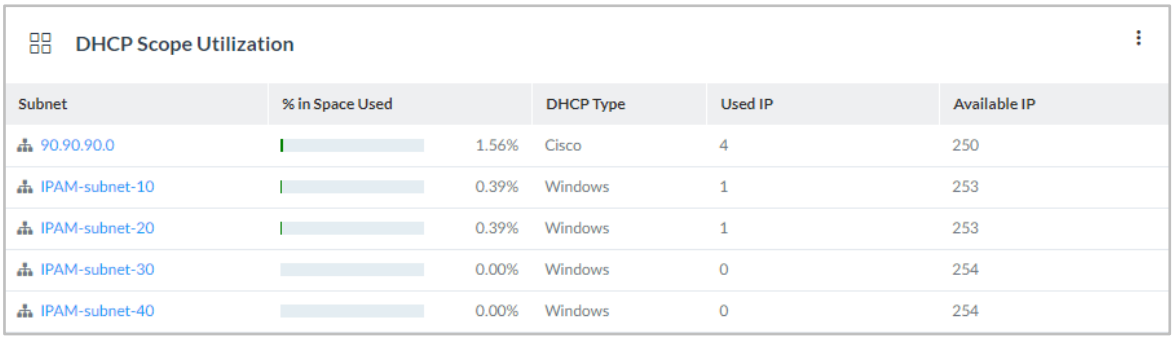


Fig 24: DHCP Scope Utilization Details

3.11. Top 10 Subnet Utilization

The widget displays the percentage of IP addresses used for the top 10 subnets. It displays the details like Subnet and % in Space Used.

Also, you can click the **More Options** icon to export the details in PDF format.

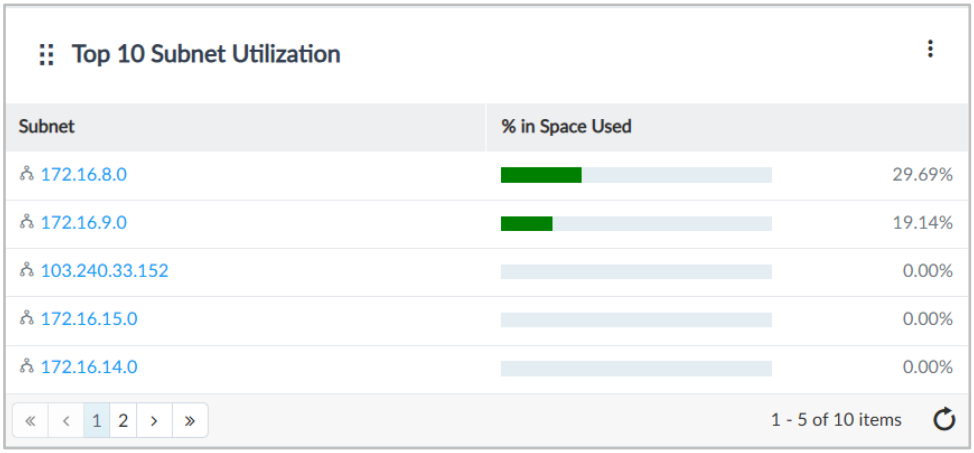


Fig 25: Top 10 Subnet Utilization

3.12. Top 10 Category Utilization

The widget displays the percentage of IP addresses used for the top 10 categories. It displays the details like Category and % in Space Used.

Also, you can click the **More Options** icon to export the details in PDF format.

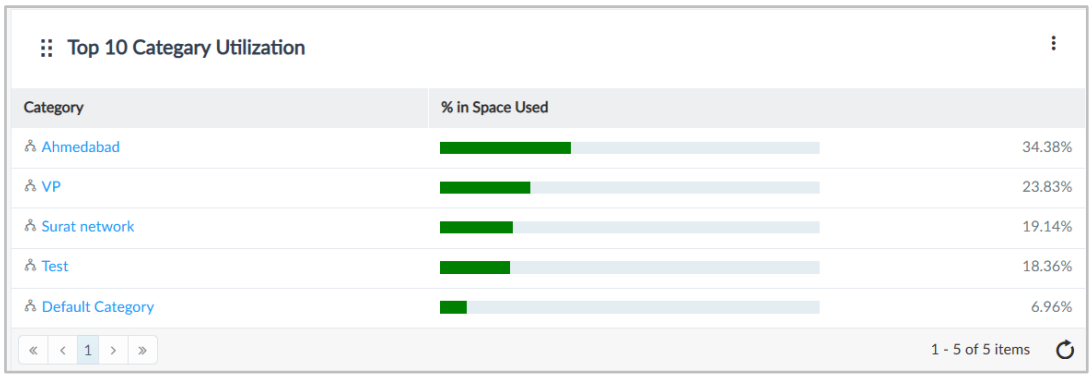


Fig 26: Top 10 Category Utilization

3.13. IP Availability Summary

The widget displays the summary of the percentage of IP addresses in a pie chart. The color coding shows the IP address status:

- **Green**: Available IP addresses
- **Yellow**: Used IP addresses
- **Blue**: IP addresses in the transient state

Also, you can click the **More Options** icon to export the details in PDF, PNG, and SVG format.

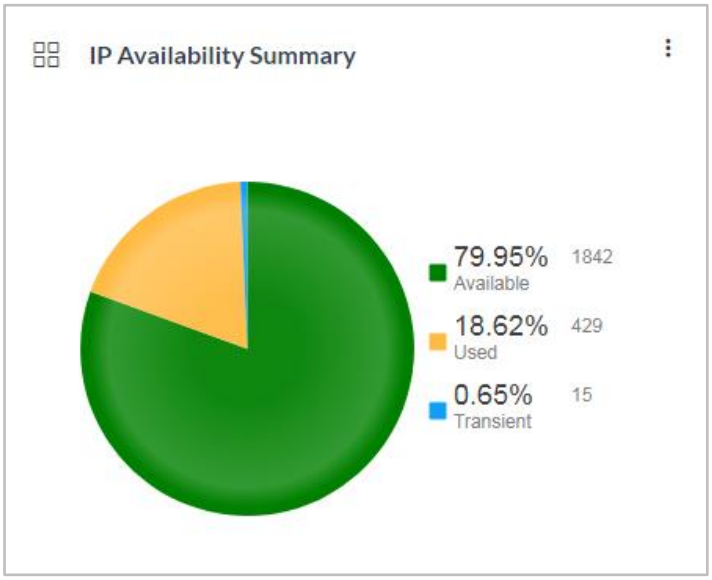


Fig 27: IP Availability Summary Graph

3.14. DNS Status Summary

The widget displays the percentage of DNS status summary in a pie chart. The color coding shows the DNS status:

- **Green**: Not available
- **Yellow**: Success
- **Blue**: Reverse Lookup Failed
- **Red**: Forward Lookup Failed
- **Purple**: Forward Lookup IP Mismatch

Also, you can click the **More Options** icon to export the details in PDF, PNG, and SVG format.

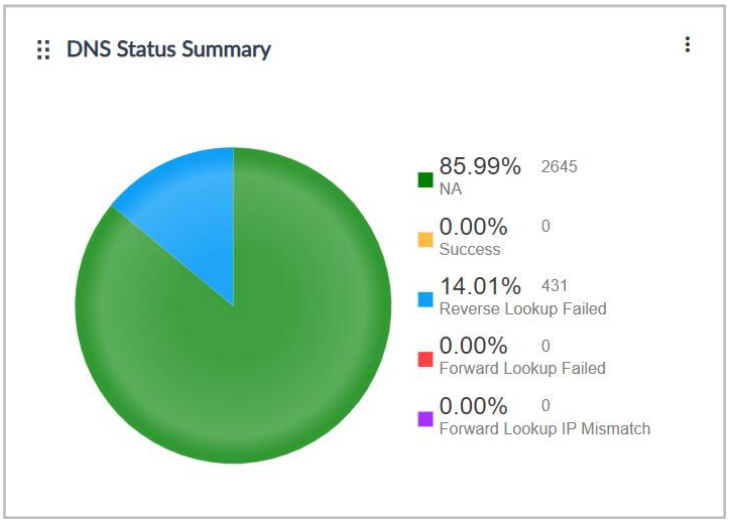


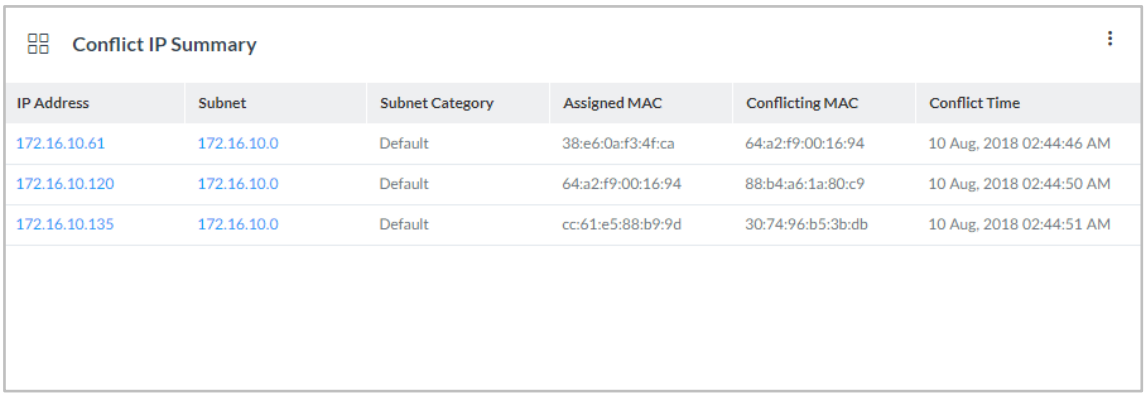
Fig 28: DNS Status Summary

3.15. Conflict IP Summary

The widget displays the list of IP addresses. An IP address is considered conflicting when one IP is assigned to a different MAC in the new scan. The widget displays the following details:

- **IP Address**: The value of the IP address
- **Subnet**: The value of the subnet to which the IP address belongs to
- **Subnet Category**: The category of the subnet
- **Assigned MAC**: The MAC address found in the previous scan
- **Conflicting MAC**: The MAC address found in the current scan
- **Conflict Time**: The time at which the conflict happened

Also, you can click the **More Options** icon to export the details in PDF format.



Conflict IP Summary

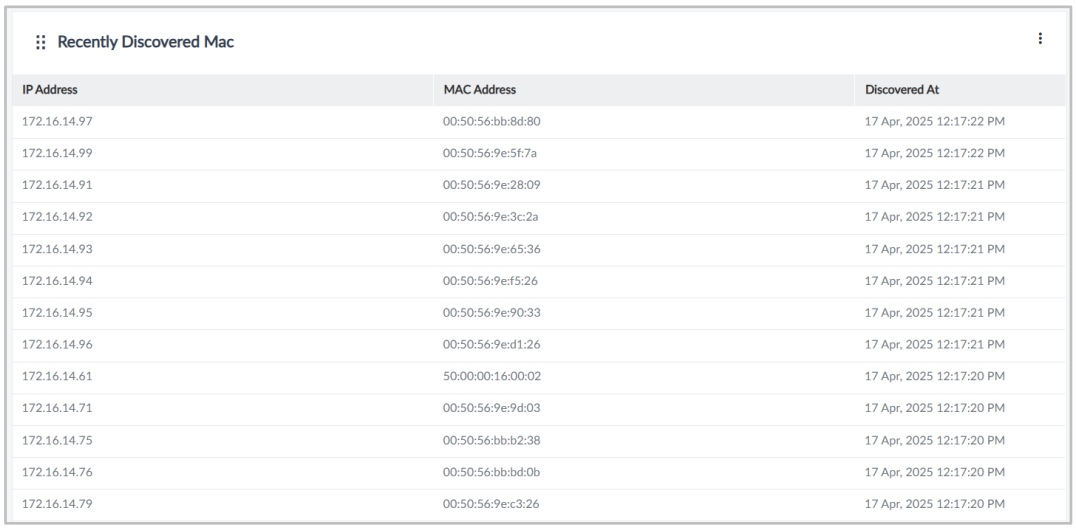
IP Address	Subnet	Subnet Category	Assigned MAC	Conflicting MAC	Conflict Time
172.16.10.61	172.16.10.0	Default	38:e6:0a:f3:4f:ca	64:a2:f9:00:16:94	10 Aug, 2018 02:44:46 AM
172.16.10.120	172.16.10.0	Default	64:a2:f9:00:16:94	88:b4:a6:1a:80:c9	10 Aug, 2018 02:44:50 AM
172.16.10.135	172.16.10.0	Default	cc:61:e5:88:b9:9d	30:74:96:b5:3b:db	10 Aug, 2018 02:44:51 AM

Fig 29: Conflict IP Summary

3.16. Recently Discovered Mac

This widget displays the details of the recently discovered MAC addresses. It consists of IP Address, MAC Address, and Discovered At timestamp.

Also, you can click the **More Options** icon to export the details in PDF format.



Recently Discovered Mac

IP Address	MAC Address	Discovered At
172.16.14.97	00:50:56:bb:8d:80	17 Apr, 2025 12:17:22 PM
172.16.14.99	00:50:56:9e:5f:7a	17 Apr, 2025 12:17:22 PM
172.16.14.91	00:50:56:9e:28:09	17 Apr, 2025 12:17:21 PM
172.16.14.92	00:50:56:9e:3c:2a	17 Apr, 2025 12:17:21 PM
172.16.14.93	00:50:56:9e:65:36	17 Apr, 2025 12:17:21 PM
172.16.14.94	00:50:56:9e:f5:26	17 Apr, 2025 12:17:21 PM
172.16.14.95	00:50:56:9e:90:33	17 Apr, 2025 12:17:21 PM
172.16.14.96	00:50:56:9e:d1:26	17 Apr, 2025 12:17:21 PM
172.16.14.61	50:00:00:16:00:02	17 Apr, 2025 12:17:20 PM
172.16.14.71	00:50:56:9e:9d:03	17 Apr, 2025 12:17:20 PM
172.16.14.75	00:50:56:bb:b2:38	17 Apr, 2025 12:17:20 PM
172.16.14.76	00:50:56:bb:bd:0b	17 Apr, 2025 12:17:20 PM
172.16.14.79	00:50:56:9e:c3:26	17 Apr, 2025 12:17:20 PM

Fig 30: Recently Discovered Mac

3.17. Top 10 Vendor Summary

The widget displays the list of the top 10 vendors from all the available vendor names of IP addresses with the count. Moreover, you can click More Options ⋮ to download the details in the PDF, PNG, and SVG format.

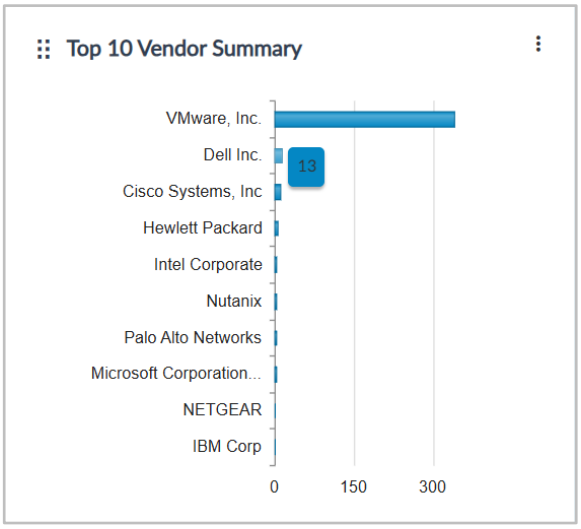


Fig 31: Top 10 Vendor Summary

4. Detailed Subnet Summary

After adding any subnet or DHCP, you can get the scope utilization on the home page. To see additional details about the subnet or DHCP, click on the name of the subnet or DHCP. IPAM will redirect you to 'Subnet Summary'. The page displays:

- Subnet Summary
- IP Addresses List

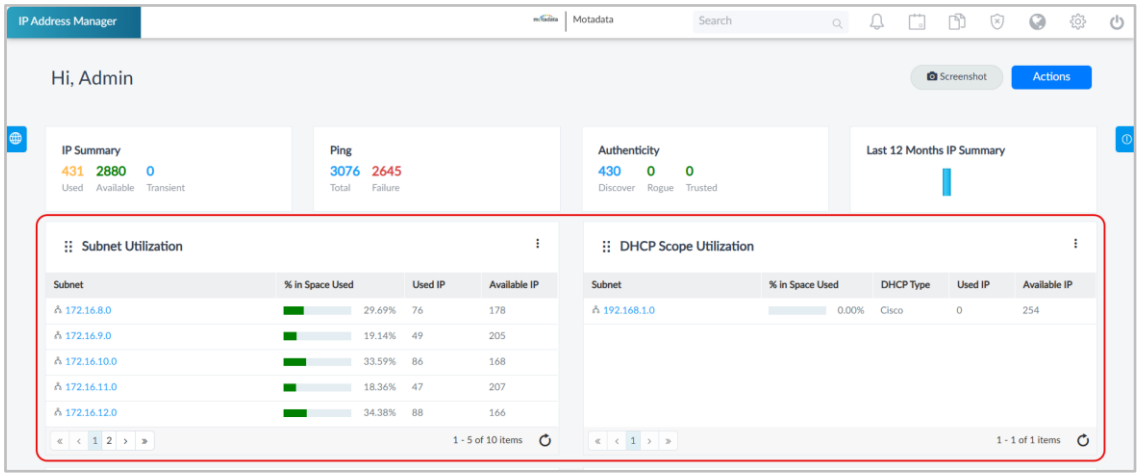


Fig 32: Homepage Showing Subnet Server

Click on the subnet name or DHCP server to go to the details page.

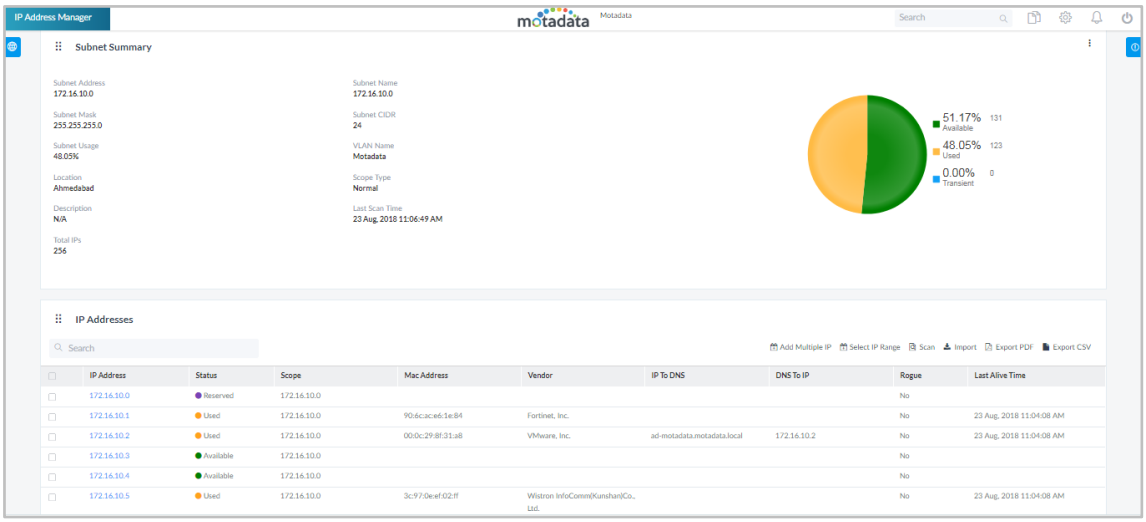


Fig 33: Subnet Details Page

4.1. Subnet Summary

The Subnet Summary displays key details of the subnet, most of which are based on the information provided during manual subnet creation (see Section – Manual Add for field details). In addition, the summary includes the following information:

- **Scope Type**: When the subnet is added manually or by importing CSV, the scope is normal. For the DHCP server case, the scope is either Windows or Cisco.
- **Last Scan Time**: The field displays the subnet's last scan.
- **Total IPs**: The field displays the total IP addresses in the subnet.

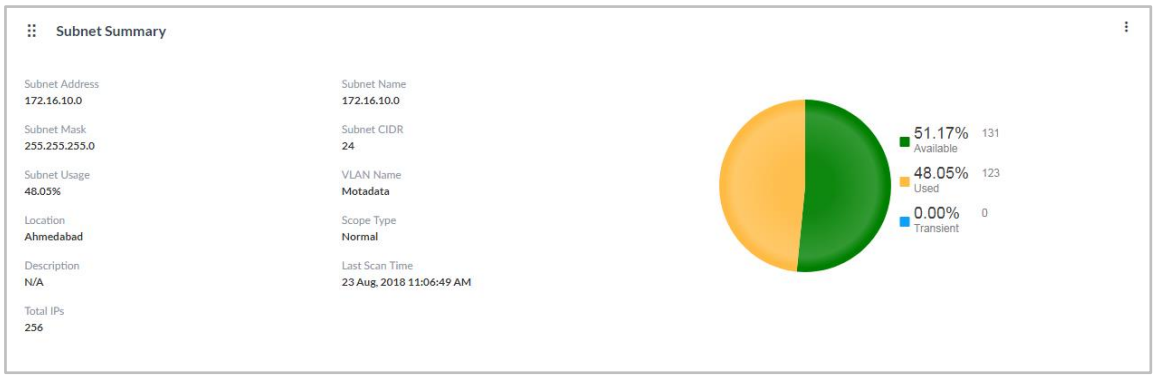


Fig 34: Subnet Summary

You can edit and delete the subnet by clicking the More Options / icon in the top-right corner.

4.2. IP Addresses

This section displays the list of IP addresses available in the subnet and the list of actions that can be performed.

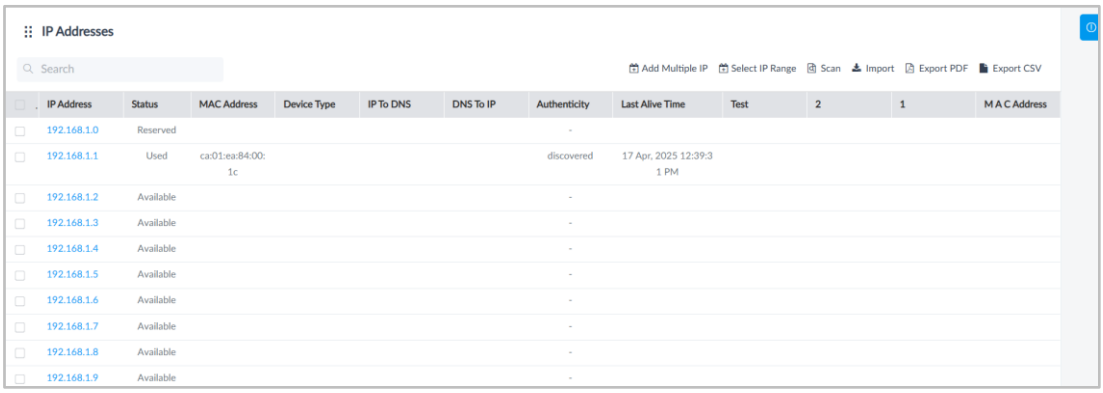


Fig 35: IP Address Actions

i. IP Address Actions

- **Search**: Type the query to search a value from the IP address table. You can search from all the columns of the table. If your search query matches a value from any column, you'll see the filtered result in the table.
- **Delete**: (Available only when rows are selected) You can delete the IP addresses through the delete option. Select one or multiple rows to delete the IP addresses.
- **Add Multiple IP**: You can add multiple IPv4 Addresses from here. You must insert the range, i.e., Start and End IP address values. IPAM will add all the IP addresses falling in that range. **This option is not available for IPv6 addresses.**

Fig 36: Add Multiple IP Addresses

- **Select IP Range**: You can manually define the IPv4 address status and remove the IPv4 address from here. This option is not available for IPv6 addresses.

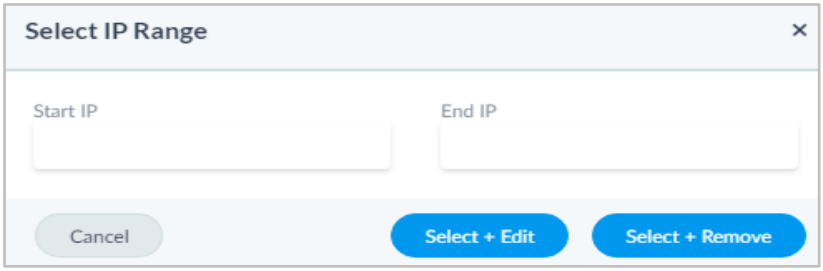


Fig 37: Select IP Range Dialog Box

To change the status of IP addresses, click the Select + Edit button, and the **Status** dropdown will become available, as shown below.

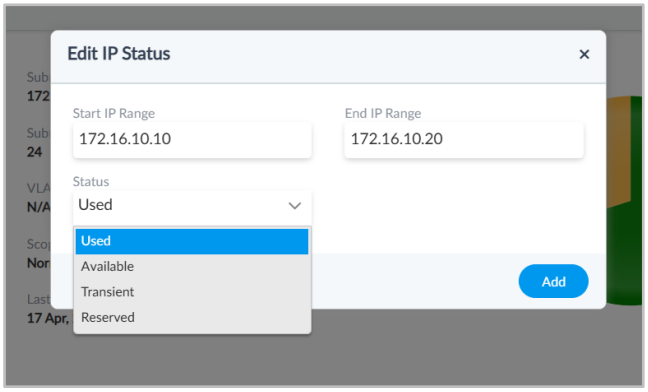


Fig 38: Set Status

You can set the status as Used, Available, Transient, or Reserved.

To delete the IP addresses, click the Select + Remove button.

- **Scan**: You can run the manual scan for the subnet using the '**Scan**' option. Scanning will update the details of IP addresses.
- **Import**: You can add an IP Address through a CSV file. To import IP addresses,
  - Click the **Import** option.
  - **Download** and use the **sample CSV** file to view columns in the supported format.
  - Fill in the details, upload the CSV file, and click **Import**.

    Note: The file should not contain IP addresses already in the IPAM system.

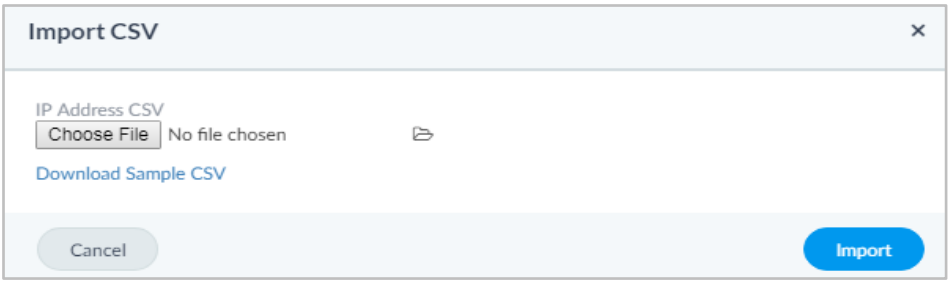


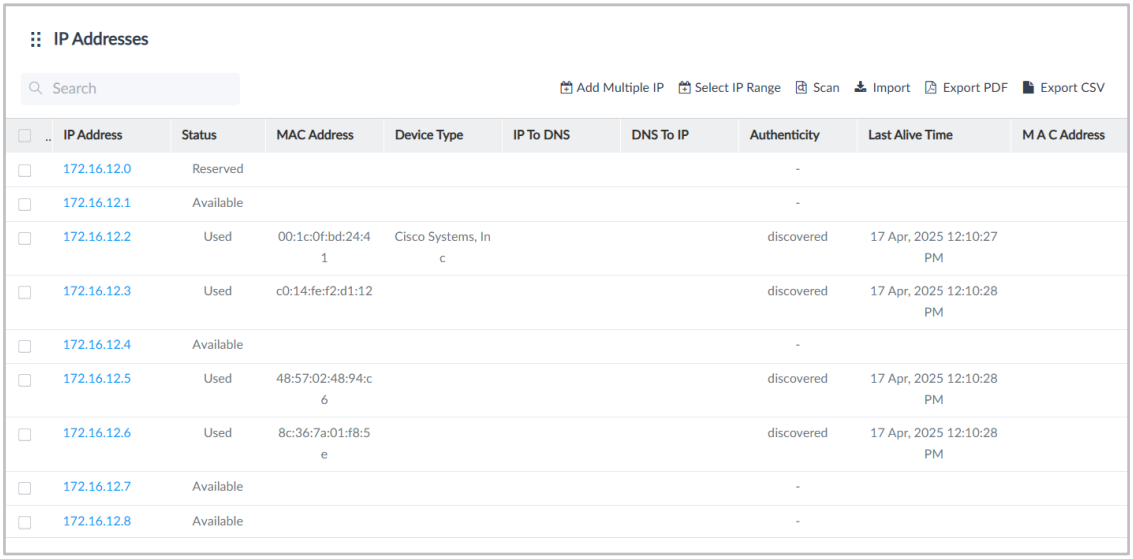
Fig 39: Import CSV Popup

- **Export PDF**: You can download the IP Address details in PDF format using Export PDF.
- **Export CSV**: You can download the IP Address details in a CSV file using Export CSV.

ii. IP Address List

This list displays all the IP addresses available in the subnet. It displays the following details about the IP addresses:

- **Status**: The column shows the current status of the IP address. The status can be Reserved (generally, the first and last IPs are reserved), Available (all new IP addresses will be available until scanned), used, and transient.
- **MAC Address**: When the IP is in a used state, the column shows the MAC address that is using the IP.
- **Device Type:** Displays the type of devices.
- **IP to DNS**: The column shows the DNS value in IP to DNS routing.
- **DNS to IP**: The column shows the IP value in DNS to IP routing.
- **Authenticity**: The column shows the authenticity of the IP addresses. The values can be rogue, trusted, and discovered.
- **Last Alive Time**: The column shows the last alive time after the scan.
- **Custom Column**: The custom columns added will appear along with their values. Here, the MAC Address is the custom column.



IP Address	Status	MAC Address	Device Type	IP To DNS	DNS To IP	Authenticity	Last Alive Time	M A C Address
172.16.12.0	Reserved					-		
172.16.12.1	Available					-		
172.16.12.2	Used	00:1c:0f:bd:24:41	Cisco Systems, Inc			discovered	17 Apr, 2025 12:10:27 PM	
172.16.12.3	Used	c0:14:fe:f2:d1:12				discovered	17 Apr, 2025 12:10:28 PM	
172.16.12.4	Available					-		
172.16.12.5	Used	48:57:02:48:94:c6				discovered	17 Apr, 2025 12:10:28 PM	
172.16.12.6	Used	8c:36:7a:01:f8:5e				discovered	17 Apr, 2025 12:10:28 PM	
172.16.12.7	Available					-		
172.16.12.8	Available					-		

Fig 40: List of IP Addresses

Note: - To get the details of IP to DNS and DNS to IP fields, the user must select the "DNS forward and reverse lookup" checkbox along with the DNS address while adding the subnet.

iii. Individual IP Address Details

Click on the IP address value in the first column of the IP address list to see the further details of an IP address.

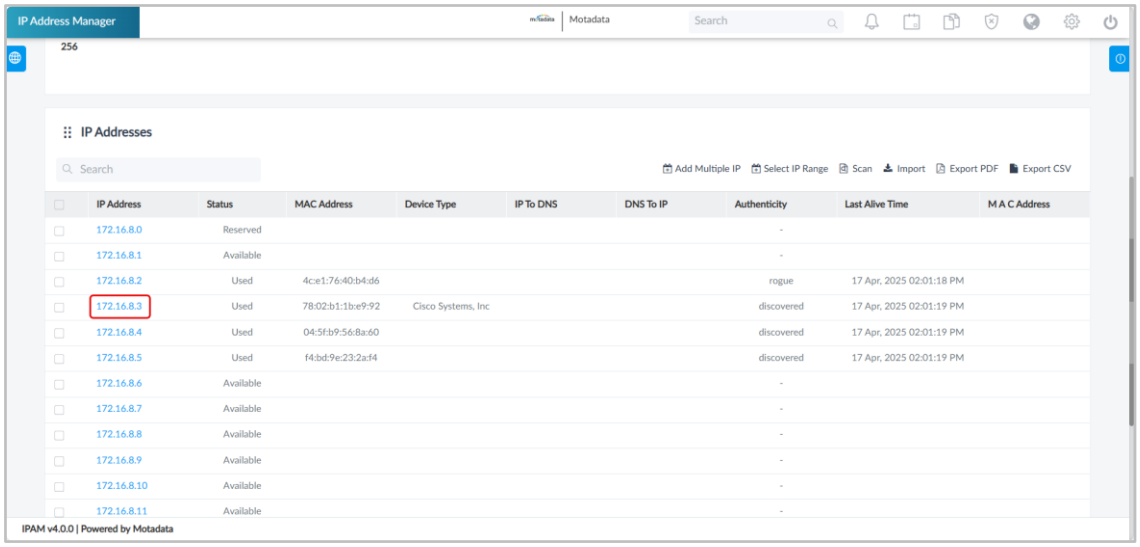


Fig 41: Click on IP Address

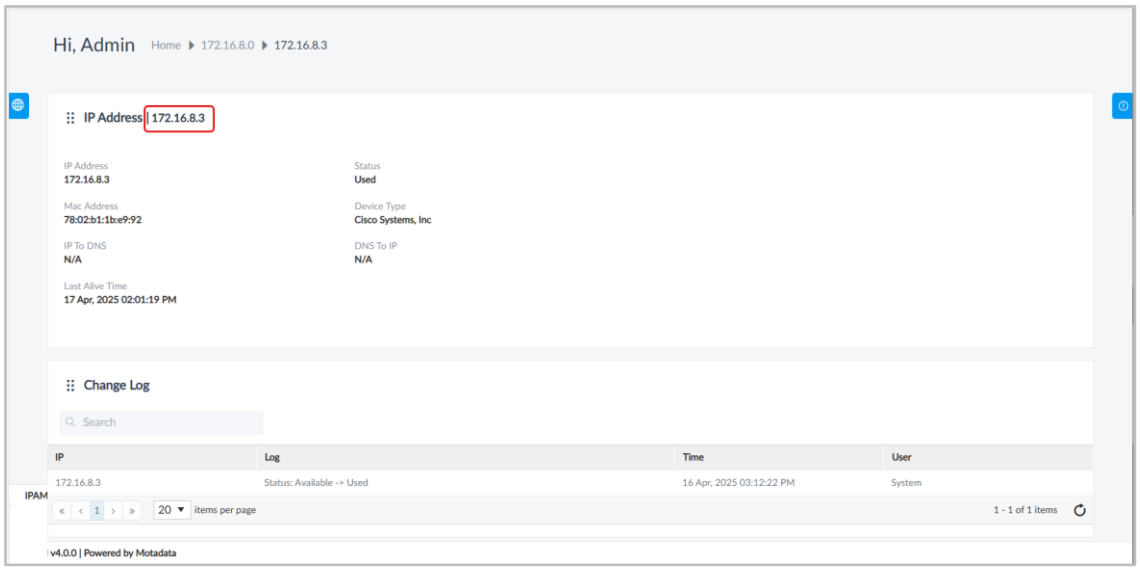


Fig 42: IP Address Details

The page displays the same details in the IP address table. You can also view the change log details on the same screen.

5. Search

The search in the system bar is a global search that finds the records of:

- Subnet Address
- IP Address
- Vendor Name

5.1. Using the Search

- Type your search query of max. 20 characters.
- The system matches your query with the database.
- The output is displayed in the tabular format.
- A maximum of 140,000 records are displayed for the given query.

6. Alerts

The alerts page displays a list of live and cleared alerts. You can also search for the required alert using the Search field.

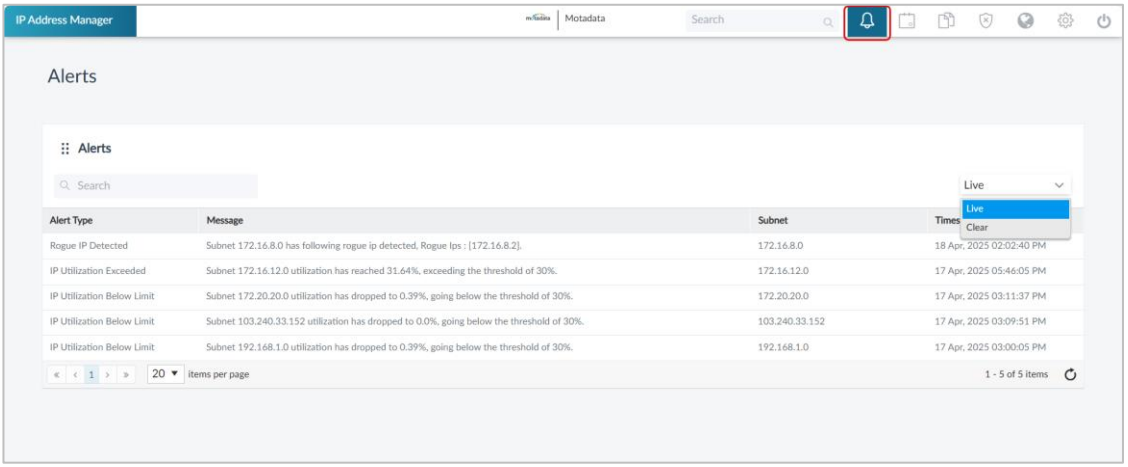


Fig 43: Alerts

7. Event Notifications

The event notifications display all the activities in the IPAM related to your IPs and DHCP server. The event is journaled automatically at your defined time. IPAM sends the event logs via email to your desired email address. IPAM generates the log for the following events:

- A new subnet is added.
- An existing subnet is deleted.
- A new user is added to IPAM.
- An existing user is deleted from IPAM.
- The user has performed the subnet and/or DHCP server scan.

- IPAM has performed the subnet and/or DHCP server scan.

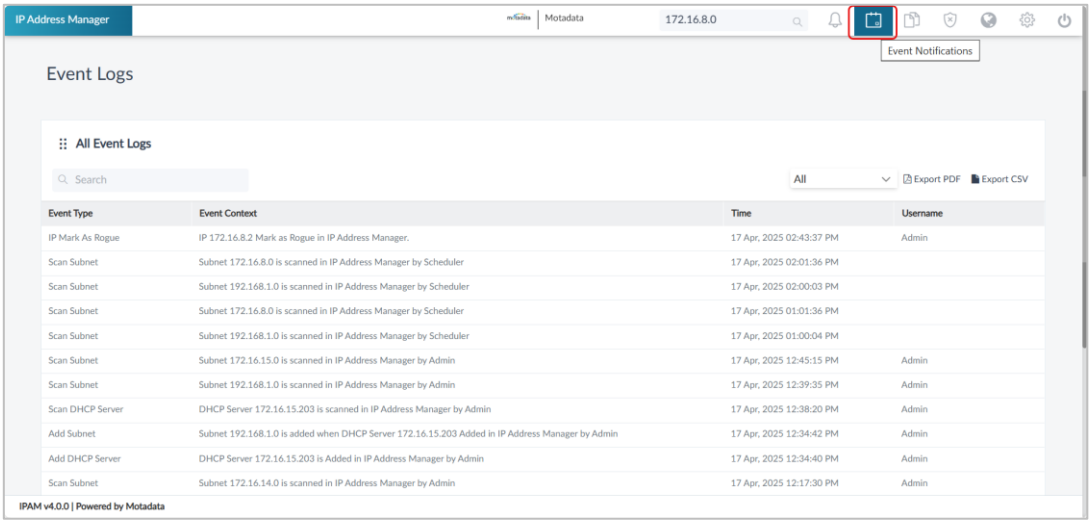


Fig 44: Event Notifications

The event notifications page displays the complete audit logs and journal entries. The logs show the following details:

- **Event Type**: The column shows the type of event that is registered.
- **Event Context**: The column shows the single-line details of the event.
- **Time**: The column shows the time at which the event happened.
- **Username**: The column shows the username of the person who performed at the event. In case the event is happened by the system, no value will be there.

You can search, filter, and export the events. You can filter the events to see the details of a particular period. Use the dropdown to select the timeframe. Also, you can export the records in PDF or CSV format.

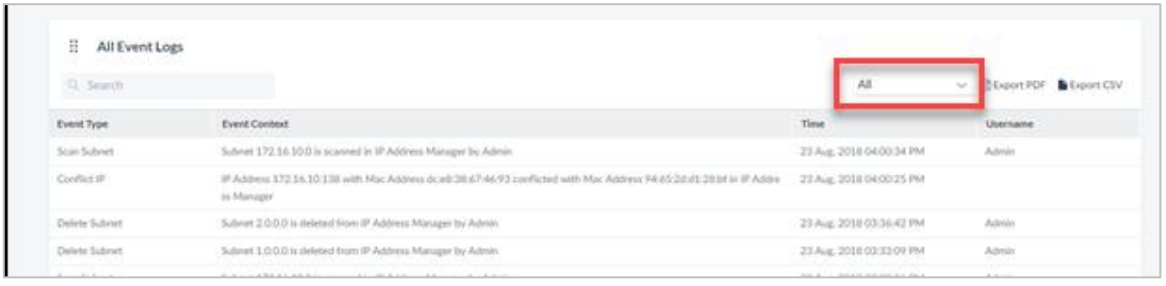


Fig 45: Select the frame for Filter

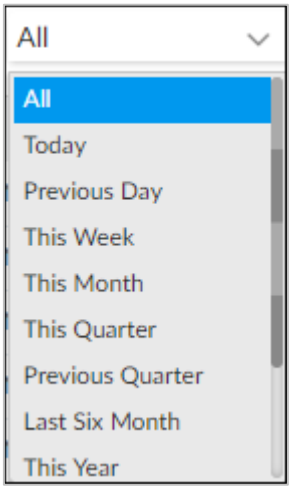


Fig 46: Timeframe for filter

8. Reports

Reports provide a comprehensive view of all IP addresses across subnets and DHCP servers. The reporting section includes various filtering options to help narrow IP information based on specific parameters. Each report can include up to 70,000 records, and the system automatically sends an email alert to the designated recipient when a report is generated.

The 'Reports' module provides various types of IP address-related reports. You can select a subnet from the left panel to view detailed information specific to that subnet.

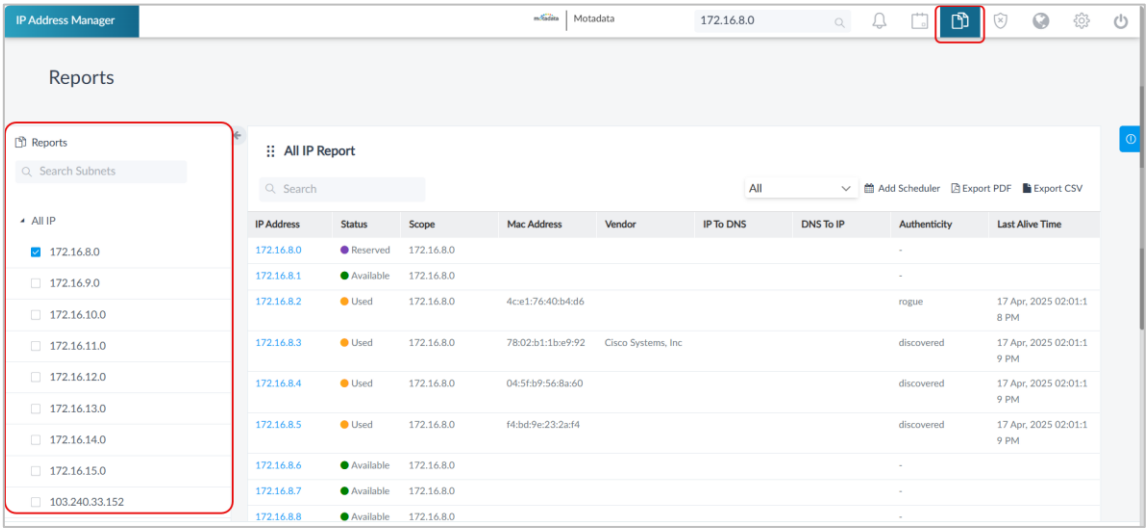


Fig 47: Reports Home Page

From the left panel, you can get reports for ALL IP, Used IP, Available IP, Reserved IP, Transient IP, Rogue IP, Trusted IP, and Vendor Summary related details. You can select multiple Subnet addresses to include in your report. The report output has an upper cap of 70,000 records.

8.1. Report Types

- **All IP**: It shows the details of IP addresses for the selected subnet address.
- **Used IP**: It shows the details of the IP addresses used for the selected subnet address.
- **Available IP**: It shows the details of available IP addresses for selected subnet addresses.
- **Reserved IP**: It shows the details of reserved IP addresses for the selected subnet address.
- **Transient IP**: It shows the details of transient IP addresses for selected subnet addresses.
- **Rogue IP**: It shows the details of rogue IP addresses for selected subnet addresses.
- **Trusted IP**: It shows the details of trusted IP addresses for selected subnet addresses.
- **Vendor Summary**: It displays the vendor's total count and the percentage of all the IP addresses for the selected subnet.

You can also schedule and export the reports as per the selected timeframe. You can export reports in PDF or CSV format. To do so,

1. Click the **Reports** icon on the System bar and open the Reports page.
2. Click the **globe** icon on the left panel and select the subnet address.
3. Select the timeframe for whose data you want to export. IP Address Manager provides (All, Today, Previous Day, This Week, This Month, This Quarter, Previous Quarter, Last Six Month, This year, Previous year, Previous Week, and Previous Month).
4. Click on the **Export PDF** or **Export CSV** option. The respective file will get downloaded. Users can now use this data to enhance their productivity.

8.2. Add Scheduler

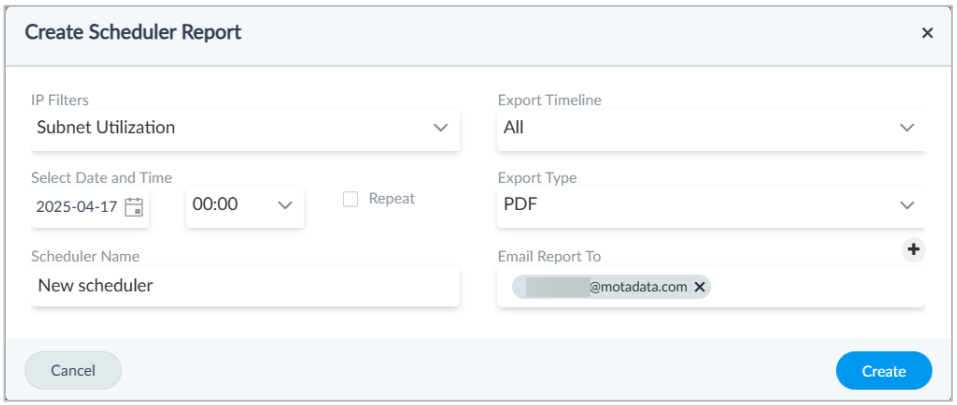
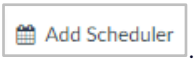


Fig 48: Create Scheduler Report

1. To schedule a report, click on 

.
2. Select an IP filter. Here, you can select the reporting for:

- All IP
- Used IP
- Reserved IP
- Transient IP
- Available IP
- Event Log
- Rogue IP
- Conflict IP
- DHCP Utilization
- Subnet Utilization
- Vendor Summary

3. Select the timeline (All, Today, Previous Day, This Week, This Month, This Quarter, Previous Quarter, last Six Month, This year, Previous year, week and Month)
4. Select the date and time for scheduling the report. **The date and time should not be of the past.**
5. Select repeat to enable the scheduler and generate a report at an interval you defined. When you select 'repeat', two additional fields appear. Provide the repeat schedule in these fields.
   - **Scheduler Timeline**: Select when the scheduler should run: Daily, weekly or monthly.
   - **Repeat On**: Select the time from the dropdown on which the scheduler will run.
6. Enter the scheduler name.
7. Select an email ID to get report details. You can add multiple recipients. Click the '+' button to add a new email id.
8. Click Create, and the Scheduler will be created successfully.
9. Check all the available schedulers from the right-hand side panel.
10. Click the  button to see the right-hand side panel. The panel shows the schedulers present in the system. You can update and delete the schedulers.

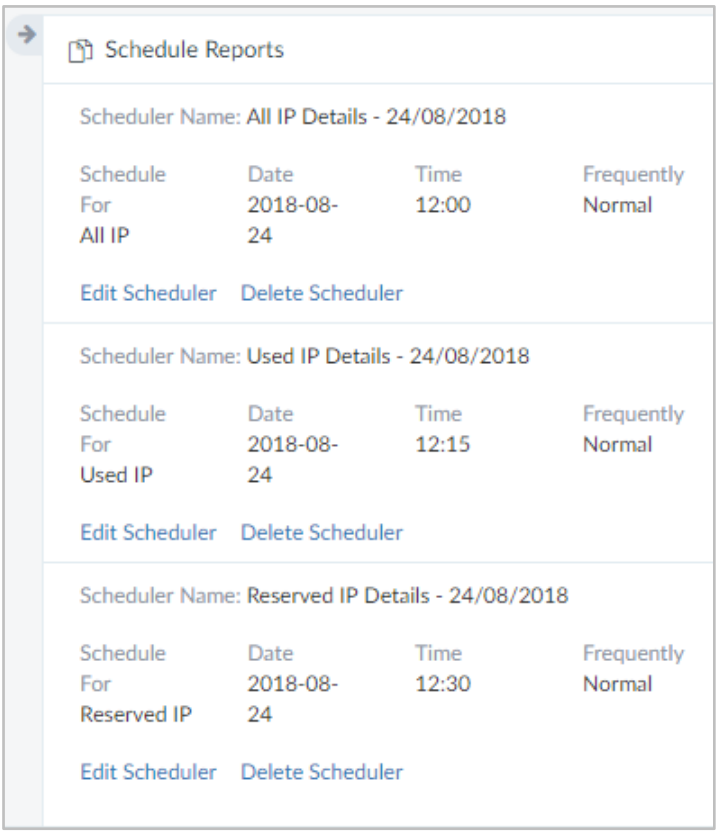


Fig 49: Schedule Reports

Field	Description
Scheduler Name	Shows the name you gave to the scheduler.
Date	Shows the first date when the scheduler will create the report.
Time	Shows the time of the day when the scheduler will create the report.
Frequently	Shows the frequency of reports. • **Normal**: When 'Repeat' is not checked in the scheduler • **Daily**: The system will generate reports daily • **Weekly**: The system will generate reports weekly • **Monthly**: The System will generate reports monthly.

9. Rogue Detection

The Rogue Detection module now provides granular control over device authenticity, allowing administrators to mark MAC addresses as Rogue or Trusted. Authenticity is dynamically determined based on MAC + IP pairing (Discovered/Rogue/Trusted) and updates automatically within the module.

To view the IP addresses, click the **Rogue Detection** icon on the System bar, and the page below will appear.

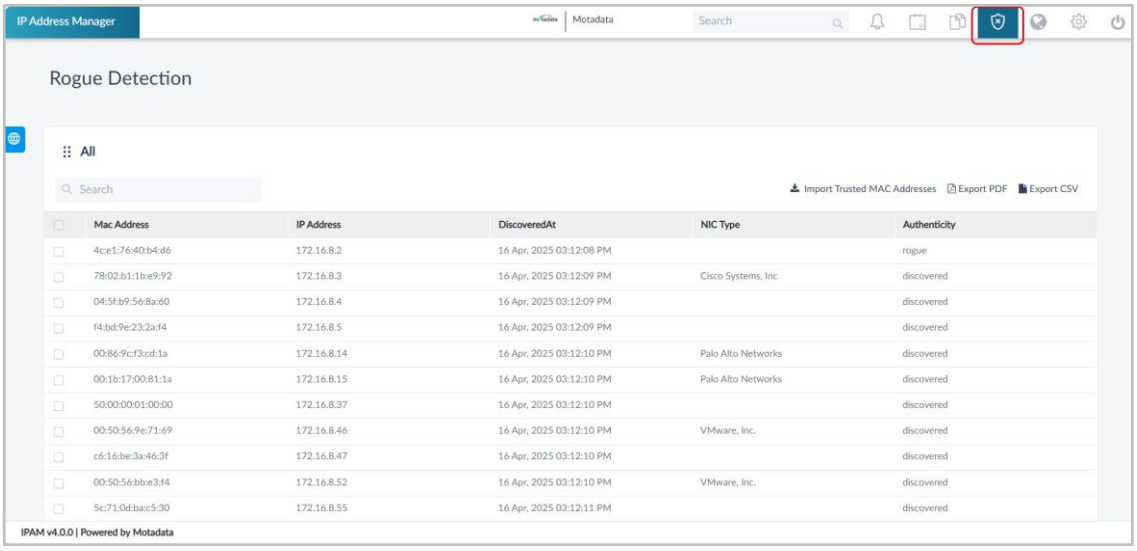


Fig 50: Rogue Detection

It displays the details below:

- MAC Address
- IP Address
- DiscoveredAt
- NIC Type
- Authenticity

Here, you can perform the below operations:

- **Search**: Type the query to search a value from the IP address table. You can search from all the columns of the table. If your search query matches a value from any column, you'll see the filtered result in the table.
- **Rogue**: (Available only when rows are selected) You can mark the scanned IP addresses as rogue or trusted using this option, as shown below.

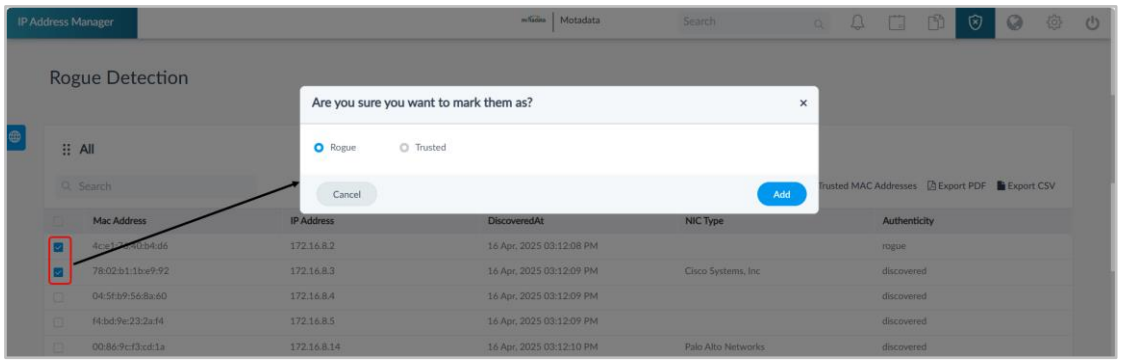


Fig 51: Mark Rogue

Once the IP Address is marked as Rogue, the same will be reflected on the Subnet Details page, Reports, etc.

- **Delete**: (Available only when rows are selected) You can delete the required IP addresses by selecting one or multiple rows. Once selected, the Delete option will become available.

  Note: Deleting a Discovered entry will remove it permanently, while Rogue/Trusted entries revert to "Discovered" instead of deletion.
- **Import Trusted MAC Addresses**: You can import the Trusted MAC Addresses in bulk. To import,
  - Click the **Import Trusted MAC Addresses** option.
  - **Download** and use the **sample CSV** file to view columns in the supported format.

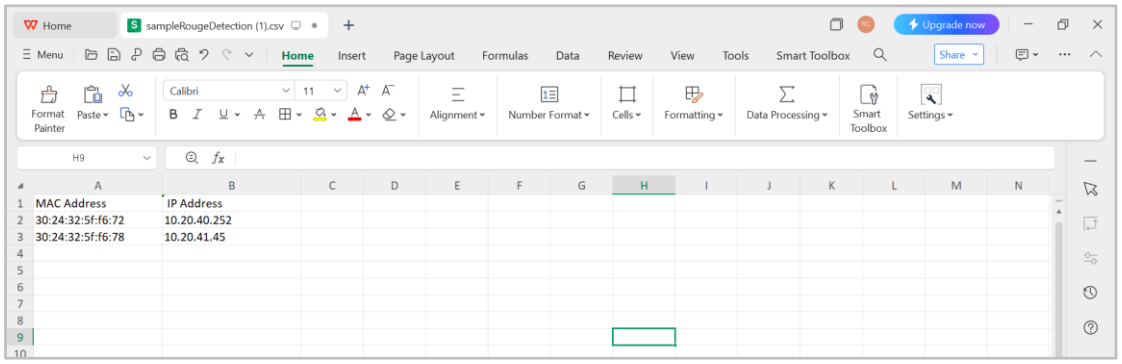


Fig 52: Sample File

- Fill in the details, upload the CSV file, and click **Import**. Once imported, the existing MACs will be updated to "Trusted," missing MACs will be added, and conflicts with rogue entries will be resolved.

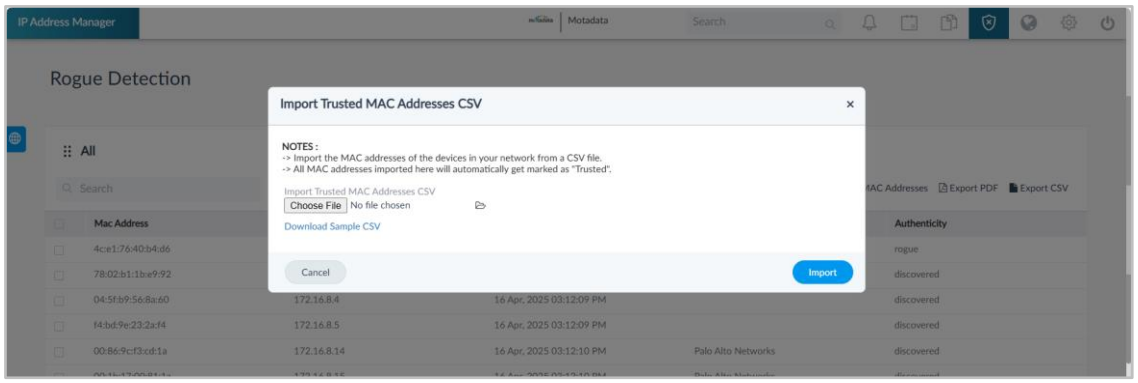


Fig 53: Import Trusted MAC Addresses

- **Export PDF**: You can download the IP Address details in PDF format using Export PDF.
- **Export CSV**: You can download the IP Address details in a CSV file using Export CSV.

10.IP Requests

The IP Requests feature in IPAM provides a streamlined and controlled process for managing IP address allocations within your organization. It allows users to formally request IP addresses, ensuring that allocations are properly tracked, approved, and conflict-free.

Users with read/write permissions can submit requests for one or more IP addresses per their requirements. These requests are then routed to administrators with the exclusive authority to review, approve, or reject them based on availability and policy guidelines.

Once an IP request is approved, the requested IP addresses are automatically marked as reserved. This prevents duplicate assignments and helps maintain accurate records of IP usage across the network.

This feature ensures better governance of IP resources, minimizes the risk of conflicts, and enhances visibility into how IPs are being allocated and utilized within the network environment.

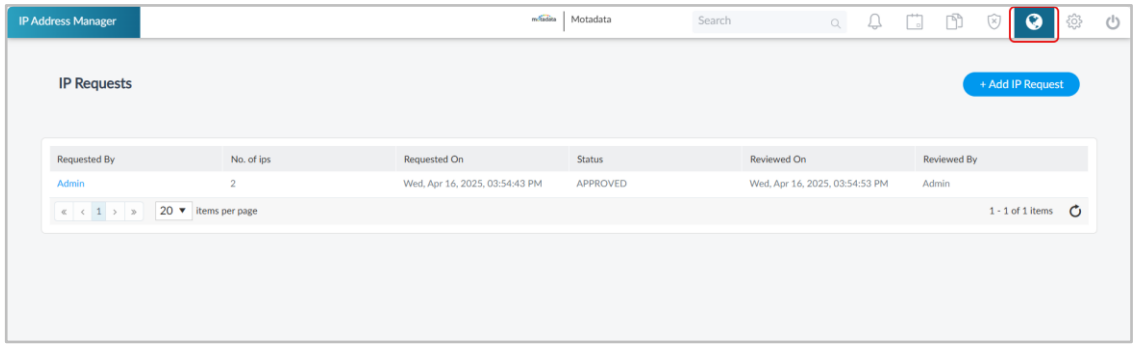


Fig 54: IP Requests

To request for IP,

1. Click the **+ Add IP Request** button, and the following popup will appear.

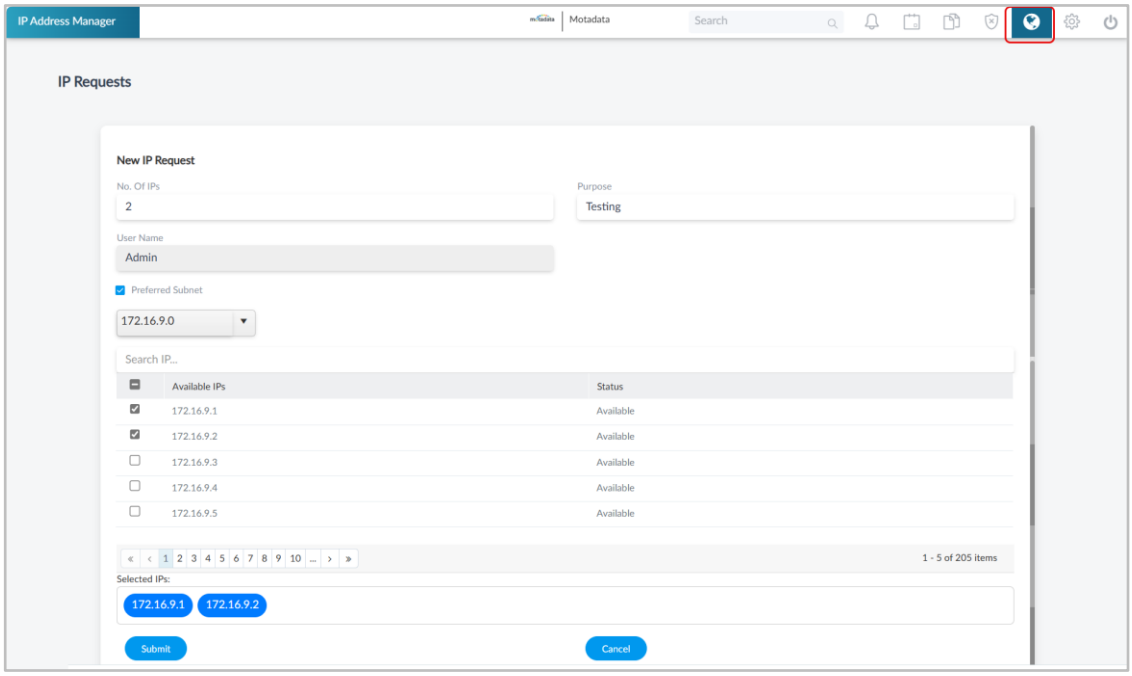


Fig 55: Add IP Request

2. Enter the below details:
   - **No. of IPs**: Enter the number of IP addresses required.
   - **Purpose**: Enter the purpose for the IP address.
   - **User Name**: Enter the username of the person to whom the request will be raised.
   - **Preferred Subnet**: If you need specific IP addresses, enable this option and select the desired IP Addresses from the dropdown.
3. Once done, click **Submit**. The request will be created, and its status will be set to pending.

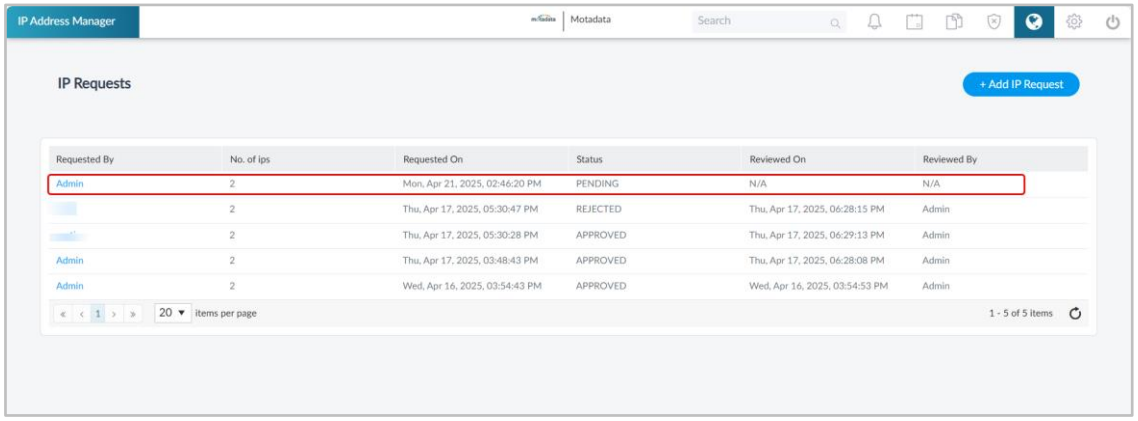


Fig 56: Newly Created IP Request

4. The Admin or any user with approval rights can click on the request to open its details page and take appropriate action. From this page, the user can either **Accept** or **Reject** the request as shown below. Upon approval, the IPs will be

automatically marked as **Reserved**, preventing any duplicate allocations. If the request is rejected, the IP address status will remain as **Available**.

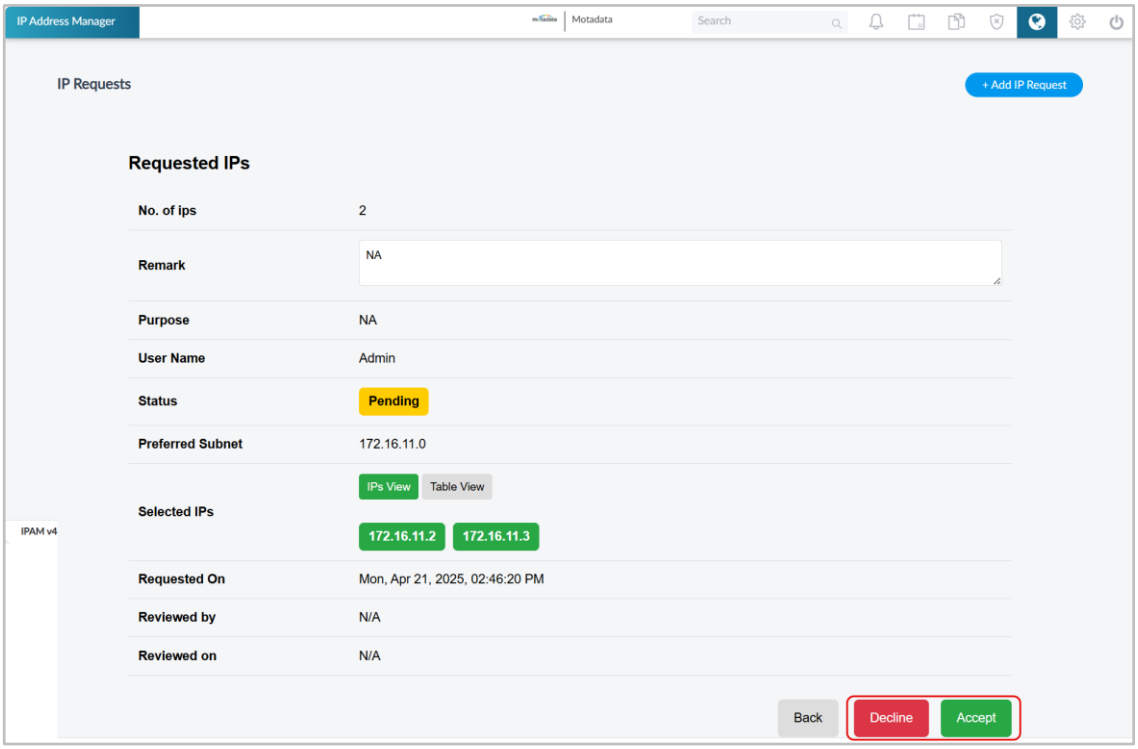


Fig 57: Accept or Reject Request

11. Settings

The settings option enables you to perform the various settings.

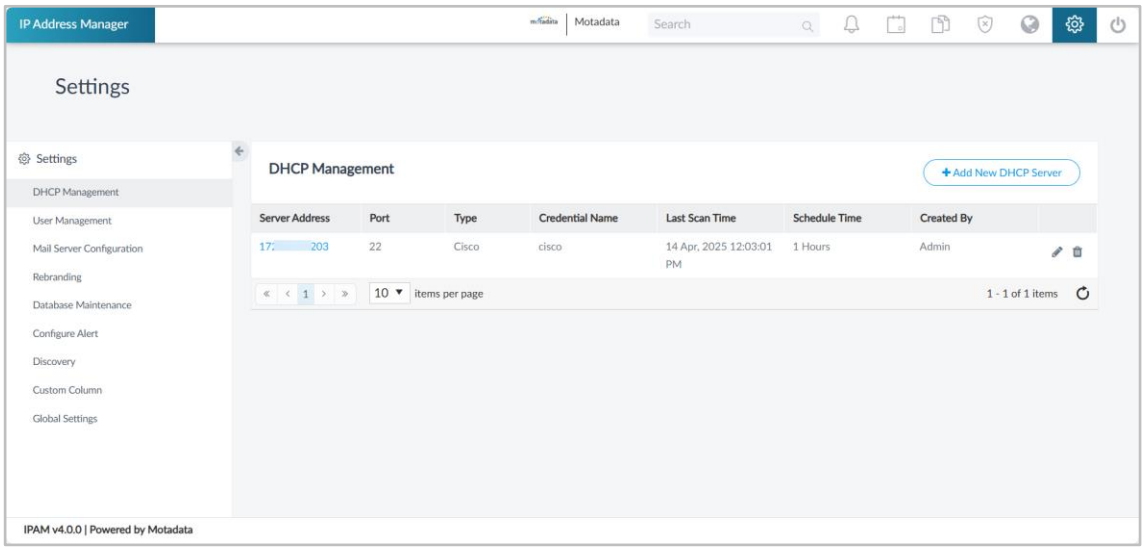


Fig 58: Settings Home Page

It includes the following sections:

- DHCP Management: Create and manage DHCP servers.
- User Management: Create and manage user accounts with access to the IPAM application.

- Mail Server Configuration: Set up email settings so IPAM can send important notifications and alerts.
- Rebranding: Customize the application's header with your logo and name.
- Database Maintenance: Control data retention settings and manage the size of your IPAM database.
- Configure Alert: Define conditions under which IPAM should send you email alerts for key events.
- Discovery: Add gateways and scan subnets automatically.
- Custom Column: Create and manage custom columns.
- Global Settings: Configure log levels and the application's theme.

11.1. DHCP Management

The DHCP Management feature provides centralized control over DHCP servers and scopes, enabling automated IP address allocation and streamlined network administration. Through the DHCP server, the user can set the reserved IP address for selected devices whenever they come into the network. This tab enables the management of the DHCP servers from a single page.

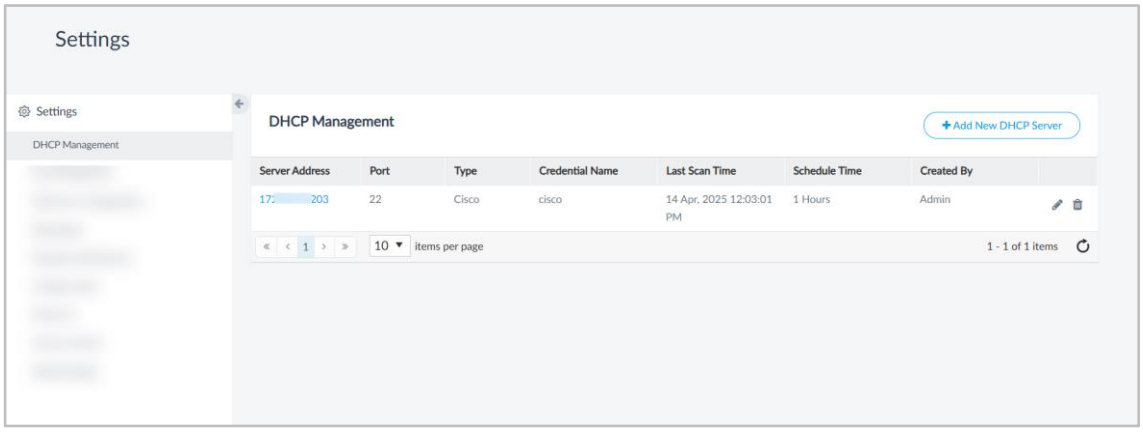


Fig 59: DHCP Management

Here, you can do the following:

- Add New DHCP Server
- View the DHCP Details
- Edit DHCP Server
- Delete DHCP Server

Add New DHCP Server:

To add a new DHCP Server, follow the below steps:

1. Navigate to **Settings > DHCP Management** and click the **Add New DHCP Server** button. The following screen appears.

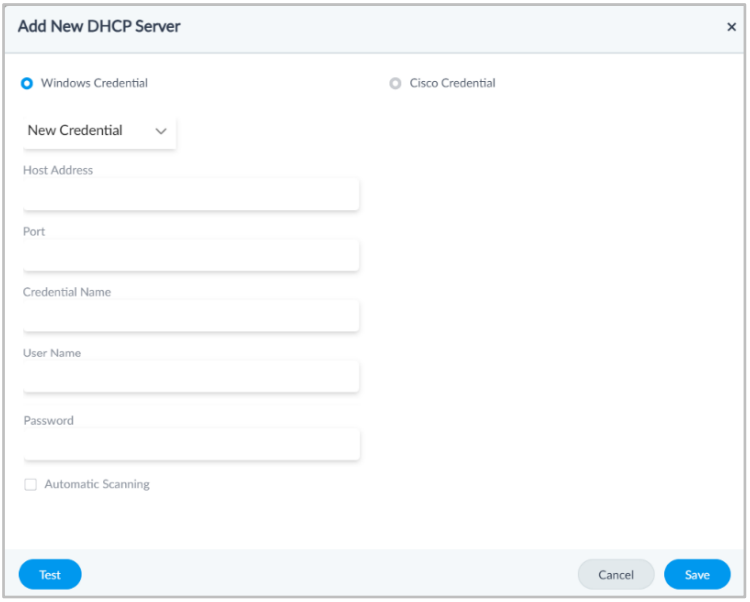


Fig 60: Add New DHCP Server

Here, you can create a DHCP Server with two types of credentials:

- Windows Credential
- Cisco Credential

Windows Credential

To add a Windows Credential, select this option and provide the below details:

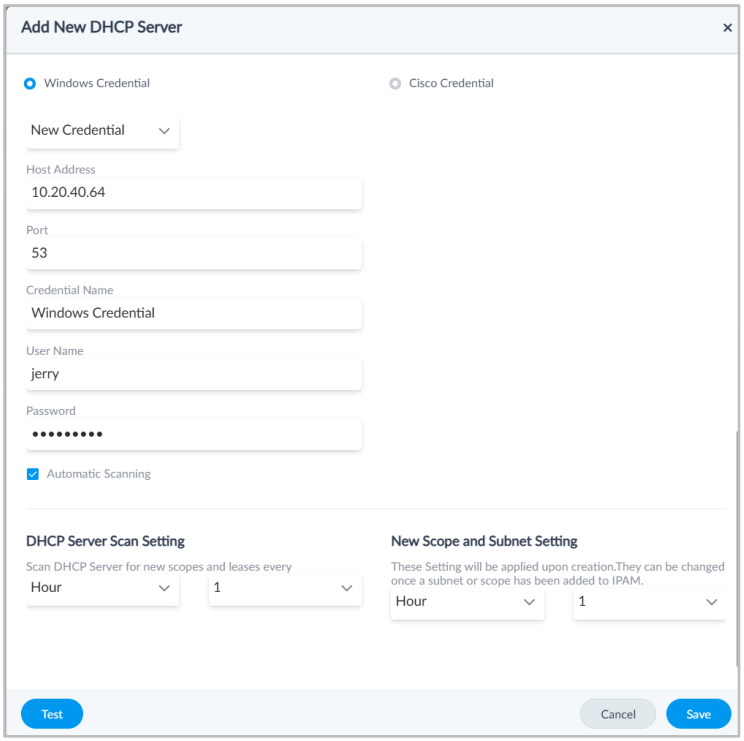


Fig 61: Add Windows DHCP Server

- **New Credential**: Select to create a new DHCP server.
- Enter a valid **Host Address**. **e.g.** 192.168.0.0
- Enter **Port**. **e.g.,** 5985
- Enter **Credential Name**.
- Enter a valid **Username**. **e.g.,** the username of Windows DHCP server
- Enter a valid **Password**. **e.g.,** Password of Windows DHCP server
- **Automatic Scanning**: You can enable the 'Automatic Scanning' or manually scan the Subnet later. For automatic scanning, check  true. Select the timeframe (Day/Week/Month) and the value. The system will run a thread to scan the Subnets automatically on the given time period.

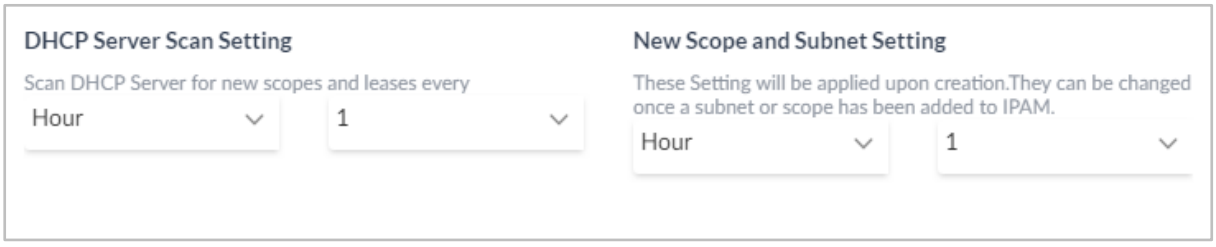


Fig 62: DHCP Automatic Scan Time Configuration

- Once done, Test the validity of your Subnet IP and DNS address. If the test is successful, the system will show a green prompt.
- **Save** the configuration.

Cisco Credential

To add Cisco Credential, select the option and provide the below details:

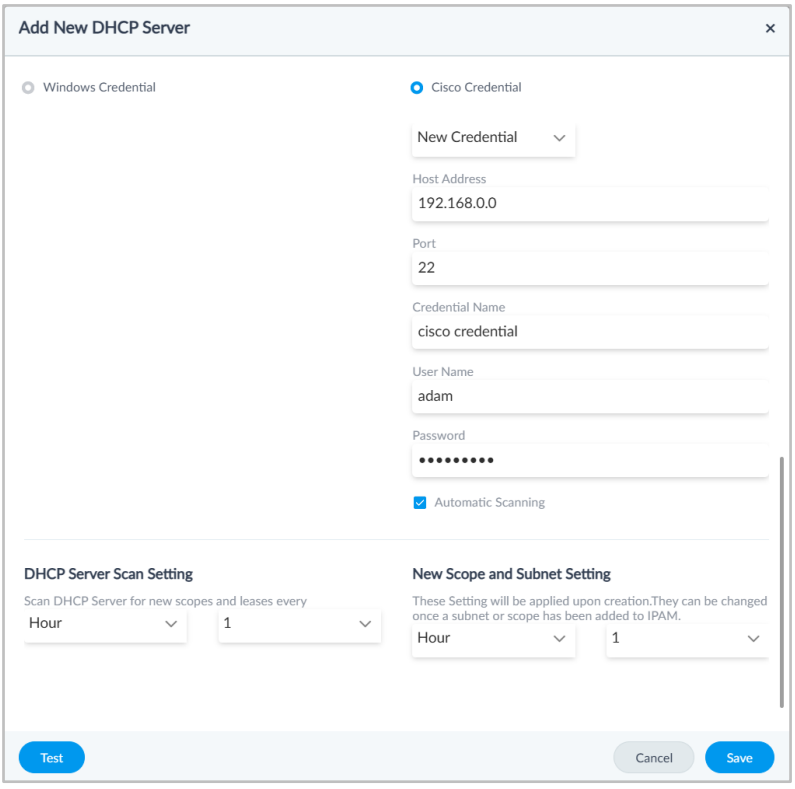


Fig 63: Add CISCO DHCP Server

- Enter a valid Host Address. **e.g.** 192.168.0.0
- Enter Port. **e.g.** 22
- Enter Credential Name.
- Enter a valid Username. **e.g.,** the username of the Cisco DHCP server
- Enter a valid Password. **e.g.,** the username of the Cisco DHCP server
- **Automatic Scanning**: You can enable the 'Automatic Scanning' or manually scan the Subnet later. For automatic scanning, check 

true.
- Select the timeframe (Day/Week/Month) and the value. The system will run a thread to scan the Subnets automatically on a given time period.

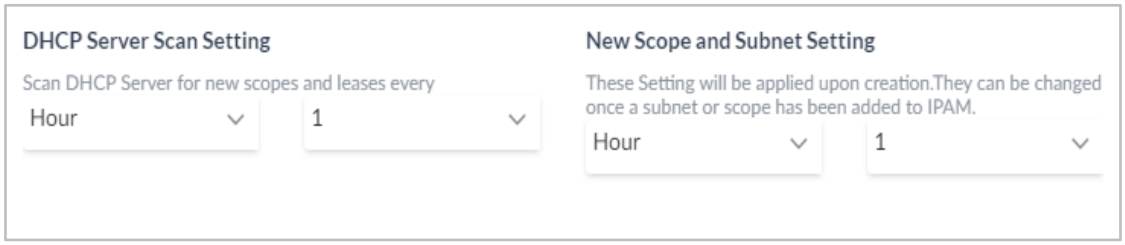


Fig 64: DHCP Automatic Scan Configuration for Cisco Server

- Once done, test the validity of your Subnet IP and DNS address. If the test is successful, the system will show a green prompt.
- **Save** the configuration.

The DHCP Server has been added and will appear on the list page. You can now perform the following operations:

- **Edit** or **delete** it if required using the respective icons.
- Refresh the list by clicking the **Refresh** icon at the bottom-right corner of the grid table.
- Set the **number of items** 10 items per page appearing on a single page. You can set 10, 20, 50, and 100. The default value is 10.

Once the credentials of the DHCP server are added, the IP Address Manager will track all the subnets present in the server. You can click on each subnet on the home page to see its details. When created, the DHCP server subnet is assigned to the 'Default' category. You can change the category later by editing the subnet.

Through DHCP management, you can view the DHCP server's summary details like Total scopes, Type of DHCP server, Declines, Offers, Requests, Discovers, Releases, ACK (acknowledgment) and NAK (negative acknowledgment) details.

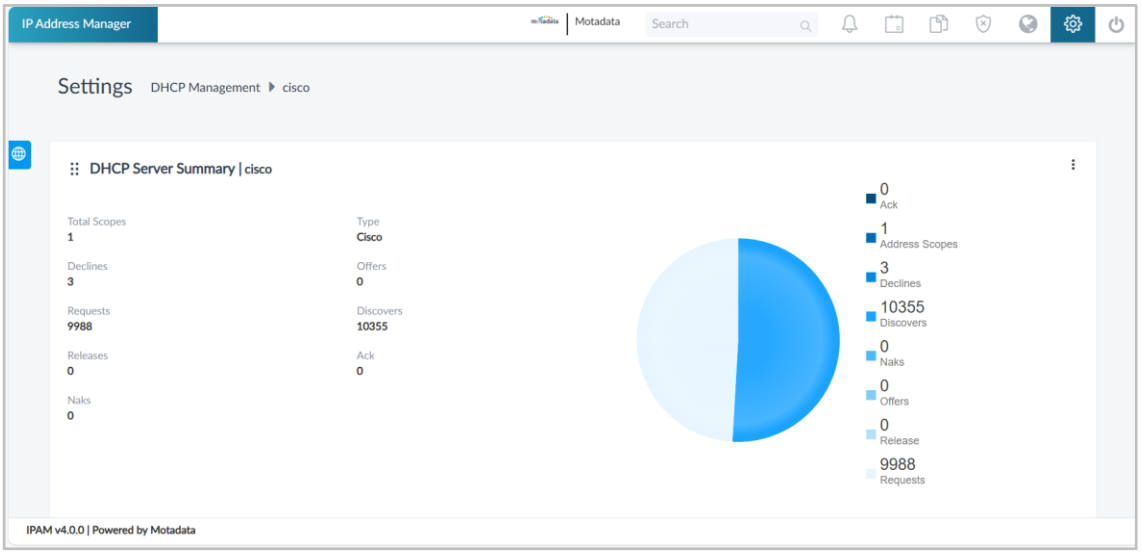


Fig 65: DHCP Server Summary

You can scan the DHCP server and export its summary details by clicking the three-dot menu in the top-right corner. The summary can be exported in PDF, PNG, or SVG format.

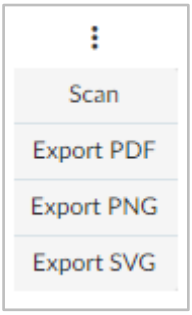


Fig 66: Export DHCP Server Summary

11.2. User Management

The User Management tab allows you to view and manage user accounts and their associated roles within the system.

- Admin users have full control and can create, update, and delete users and roles.
- Standard users have read-only access and can export user data in PDF and CSV formats.

Administrator privileges are required to add, edit, or delete users or roles,
Additionally, the Settings menu will display only the 'DHCP Management' option for non-admin users. All other settings and configuration options are hidden to maintain appropriate access controls and system security.

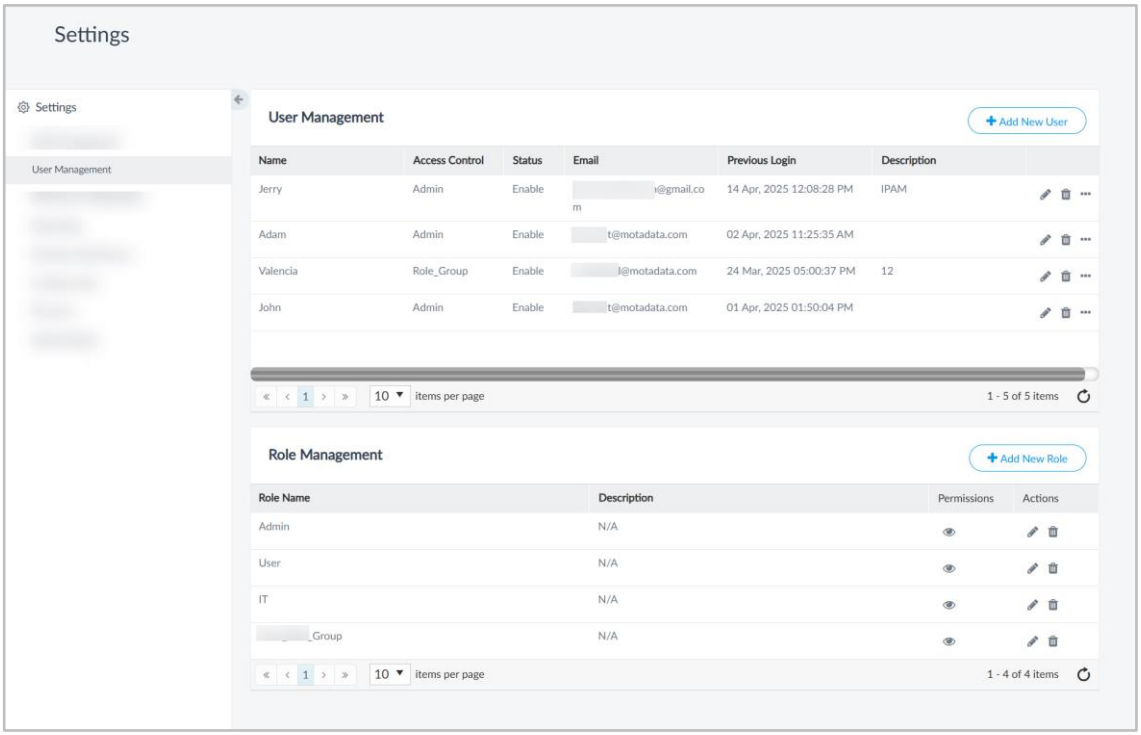


Fig 67: User Management

User Management

This section enables to view and manage the users. To create the users, follow the steps below:

1. Click 

, and the following popup appears.

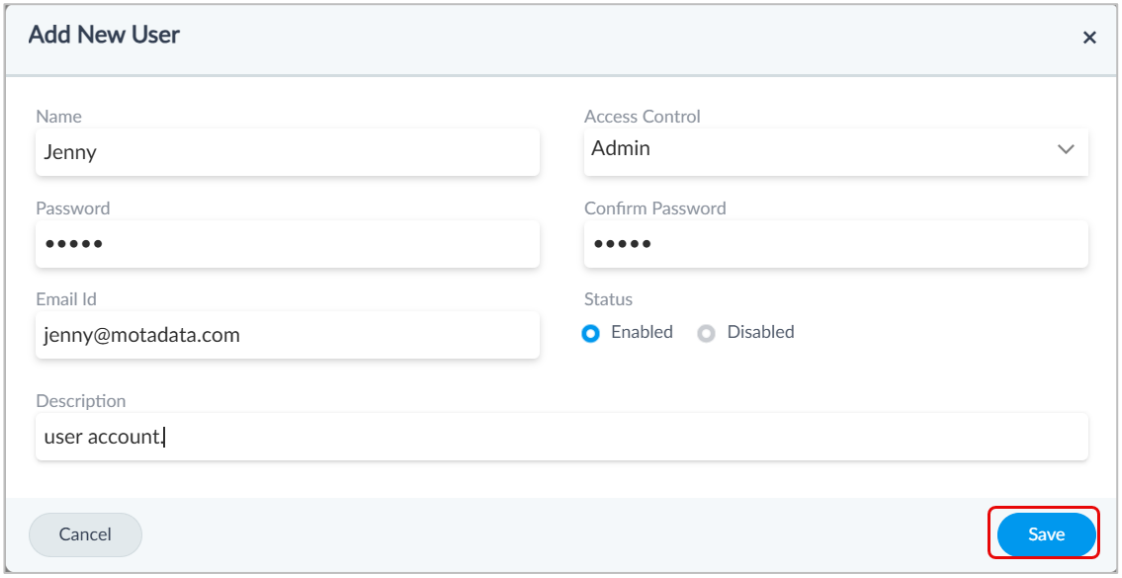


Fig 68: Create a New User

2. Enter the below details:
   - **Name:** Enter the name of the user. It is mandatory.
   - **Access control:** Select the role you want to assign to the user.
   - **Password:** Enter the password. It is mandatory.
   - **Confirm Password:** Enter the password again for confirmation.
   - **Email Id:** Enter the user's email address. It is mandatory.
   - **Status:** Select the initial status of the user as Enabled or Disabled.
   - **Description:** Enter a brief description of the user. It is Optional.
3. Once done, click **Save**.
4. You can now **edit** or **delete** the user if you no longer require it using the respective icon from the grid. Also, you can update the user's password by clicking the three dots and selecting the **Update Password** option.

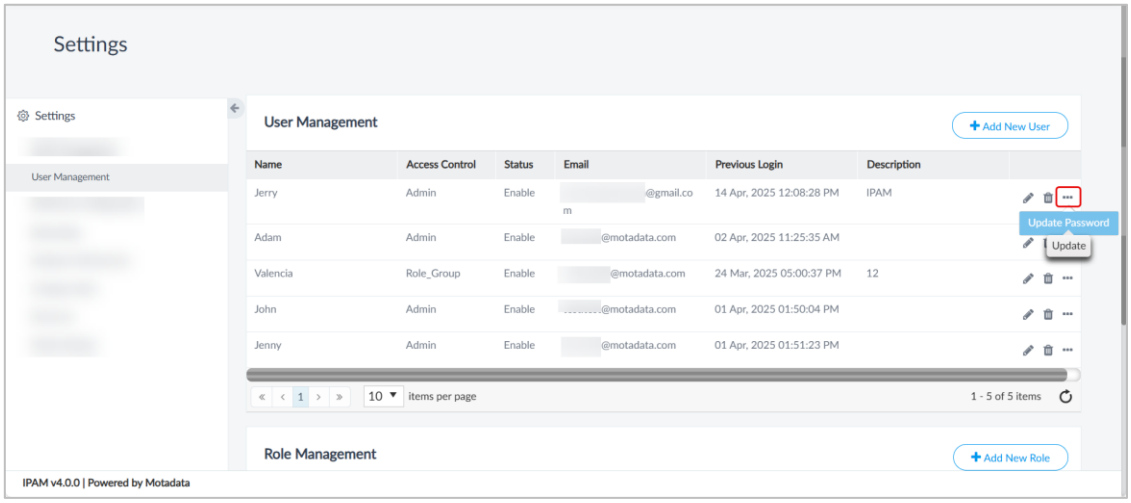


Fig 69: Update Password

Role Management

This section enables the manage the roles. To create a new role, follow the below steps:

1. Click the **Add New Role** button, and the following popup will appear.

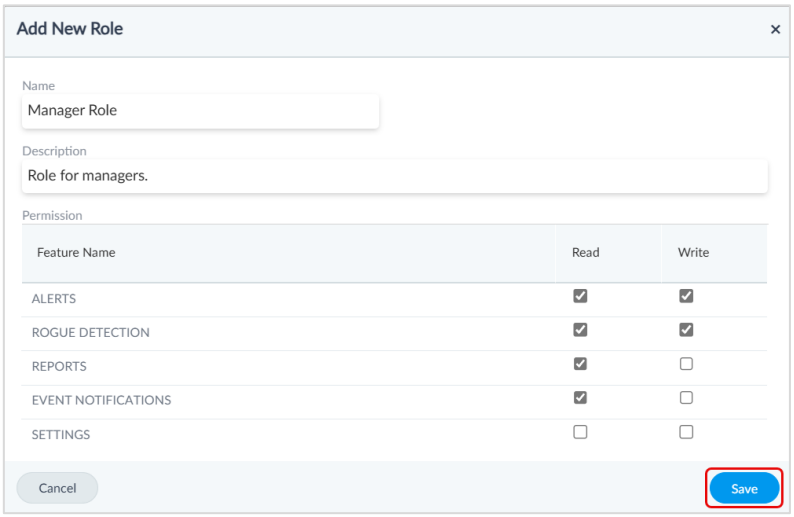


Fig 70: Add New Role

2. Enter the below details:
    - **Name**: Enter the name of the role.
    - **Description**: Enter a brief description of the role.
    - **Permission**: Select the read and write permissions for the respective feature.

3. Once done, click **Save**. The role will appear on the list below.

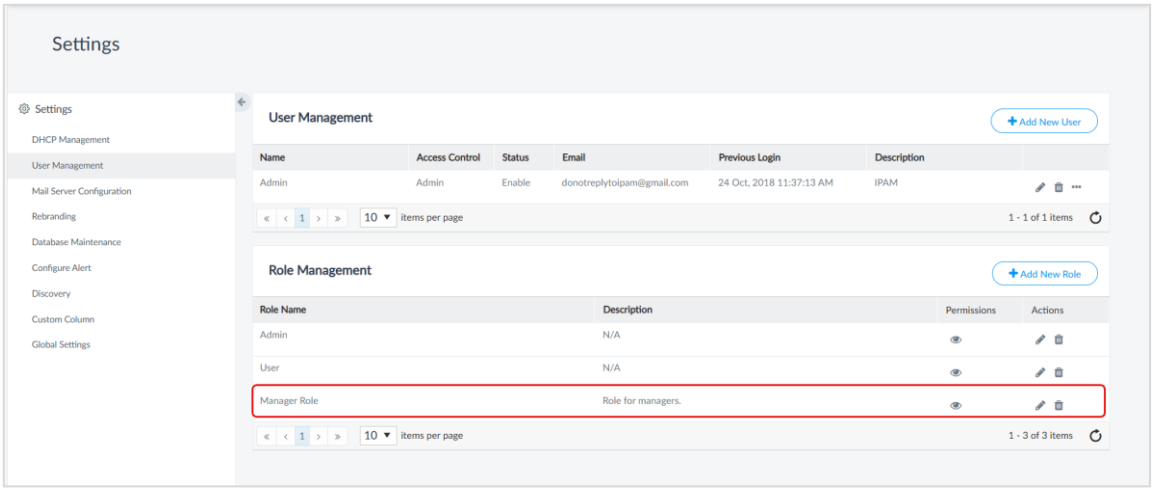


Fig 71: Created Role

4. You can now perform the following tasks:
   - **View Permissions**: Click the **eye** icon to view the feature permissions associated with the role.

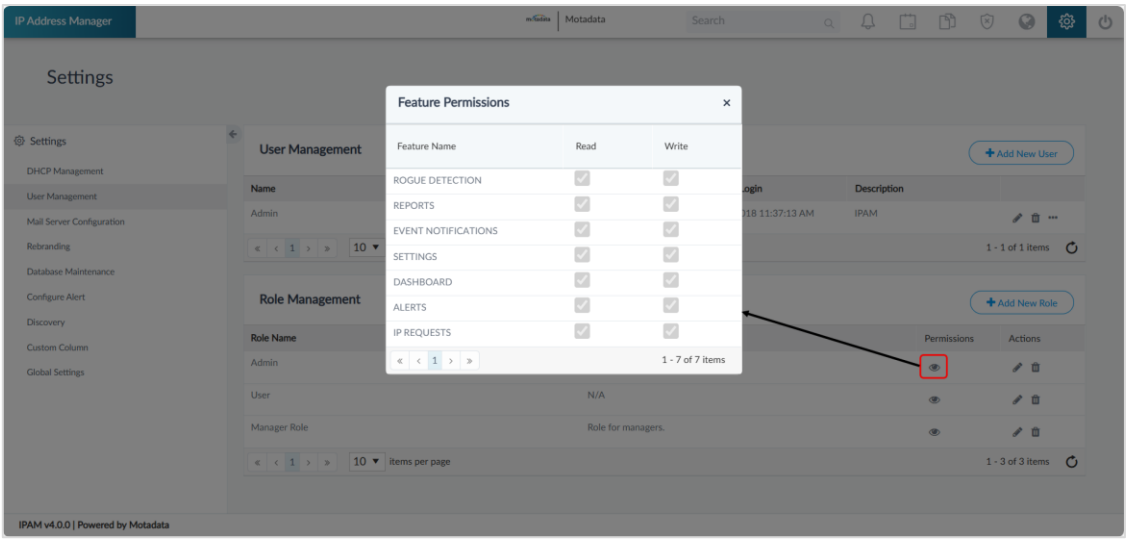


Fig 72: View Permissions

- **Edit**: Click the pencil icon to modify the permissions in the role.
- **Delete**: Click to delete the role if it is no longer required. A confirmation dialog box will appear. Click **Yes** to continue or **No** to stop the process.

11.3.Mail Server Configuration

Mail Server Configuration allows IPAM to send system-generated emails for notifications and scheduled reports. It ensures users receive timely updates, such as alerts for subnet additions or deletions and regular email-based reporting.

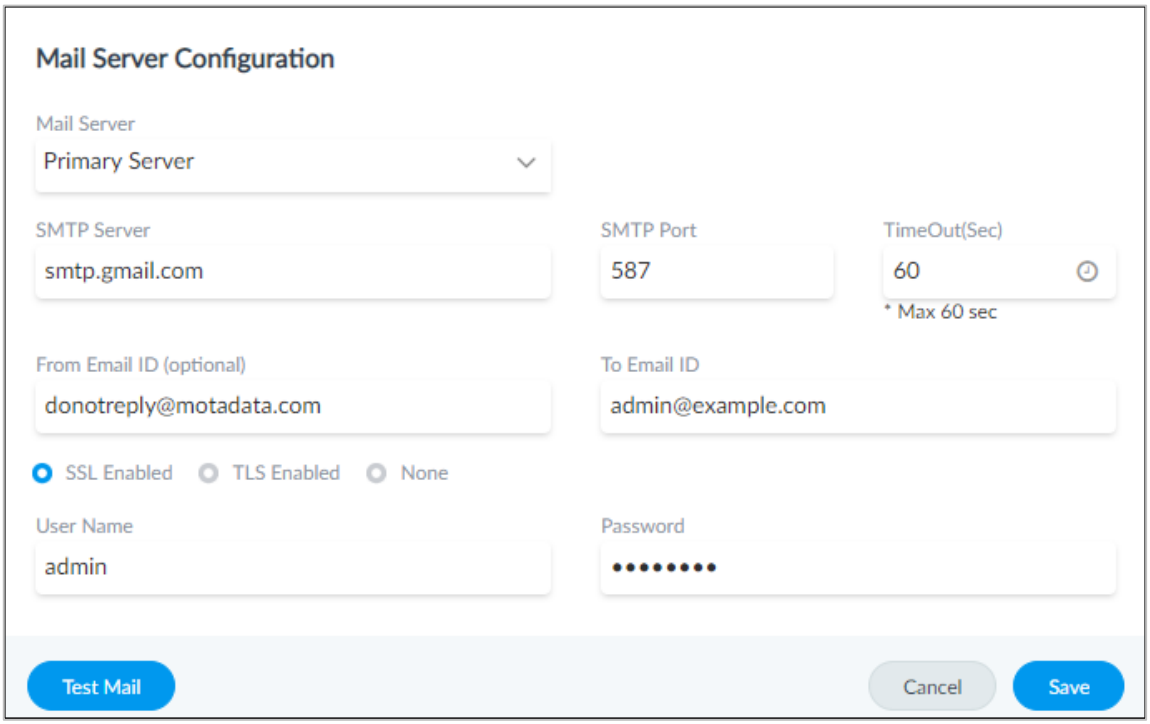


Fig 73: Mail Server Configuration

To configure the Mail Server, provide the following details:

- **Mailer Server**: Select the type of mail server you want to configure. The options are:
  - **Primary**: Select to send emails through the primary server.
  - **Secondary**: Select to send emails through the secondary server.
- **SMTP Server**: Provide the name of the SMTP Server (e.g. smtp.google.com)
- **SMTP Server Port**: Enter the SMTP server port number. (e.g., 587 for Gmail). The default SMTP Server port number is 25.
- **Timeout(second):** Enter the maximum time after which the session will timeout. The maximum value is 60 seconds.
- **Email:** Enter the from and to email addresses.
  - From Email ID
  - To Email ID
- **Security Type**: Select the type of security. SSL/TLS (e.g., SSL for Gmail)
  - SSL Enabled
  - TLS Enabled
  - None
- **Name**: Enter the user's name to which the email notification will be sent.
- **Username**: Enter the username to send the email to the recipients. This value will be displayed in the email body's first line (in greetings). (e.g. Hi, Admin)

- **Password**: Type the email id password configured as 'From Email ID'.
- Once done, click on **Test Mail** to check the connectivity with the email server.
- Once successfully connected, click **Save**.

11.4. Rebranding

You can change the logo and product name displayed on the header bar.

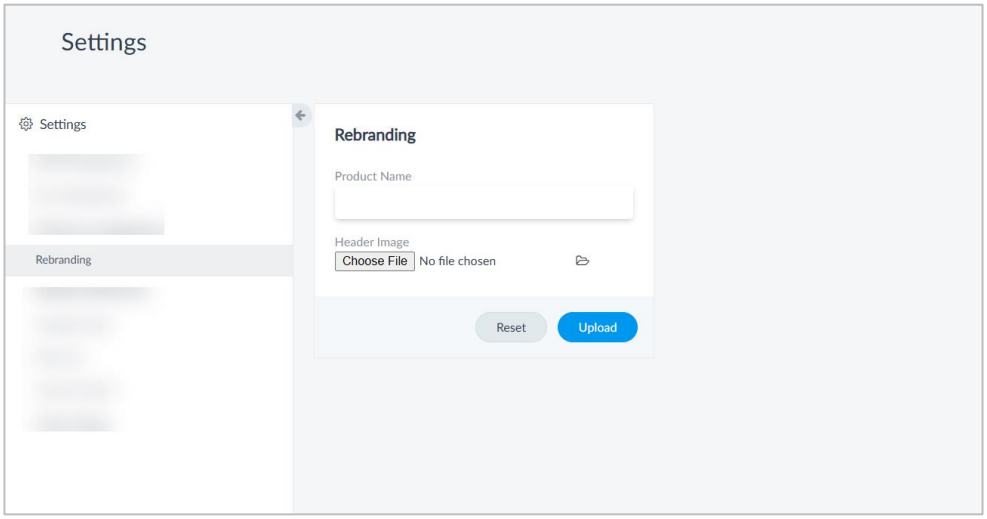


Fig 74: Rebranding Screen

11.5. Database Maintenance

Database Maintenance in IPAM helps manage and optimize database performance by providing options to view maintenance status, set data retention periods, and run archives. The page also allows users to configure regular database backups by specifying a storage path and setting a repeat schedule on a daily or monthly basis.

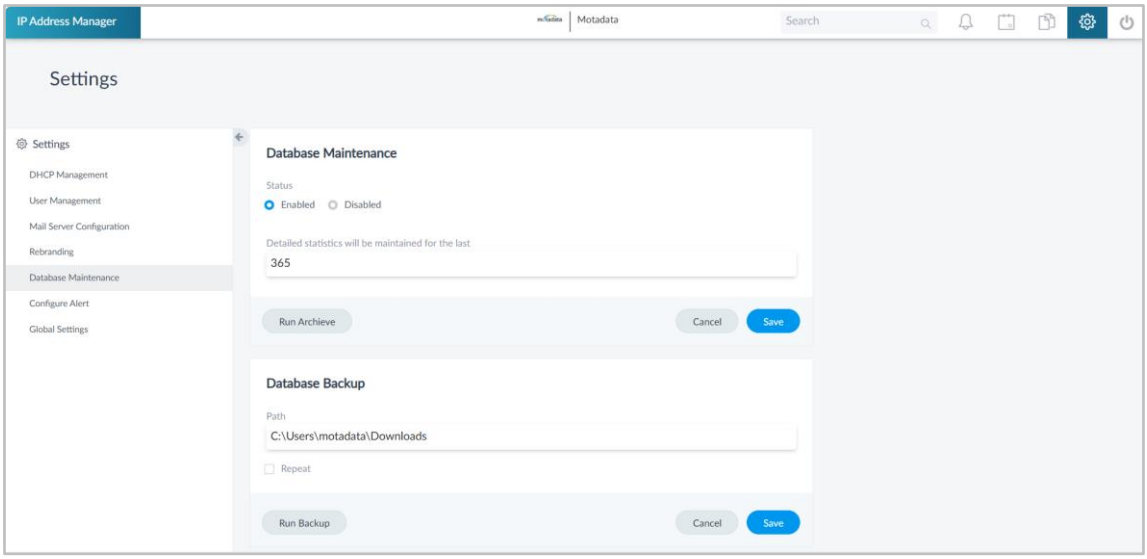


Fig 75: Database Maintenance Screen

Here, you can do the following:

- Enable or disable the database retention using the **Status** field. By default, it is enabled.

- IPAM keeps the database of the last 365 days (by default).
- You can also specify the path for storing database backups and schedule them to run daily or monthly.

11.6. Configure Alert

Configure Alert allows users to set up notifications for critical events within IPAM. Users can define alert conditions, choose notification methods, and ensure timely awareness of important changes or issues in the IP address infrastructure.

Notes:

- Only subnet-level alerts are shown in the UI (Rogue Detection, IP Utilization Exceeded, IP Utilization Below Threshold).
- IP conflict and MAC-IP alerts will not be applicable when uploading a CSV from the UI.
- MAC-IP alerts are only generated if a MAC-IP pair is present in rogue detection.

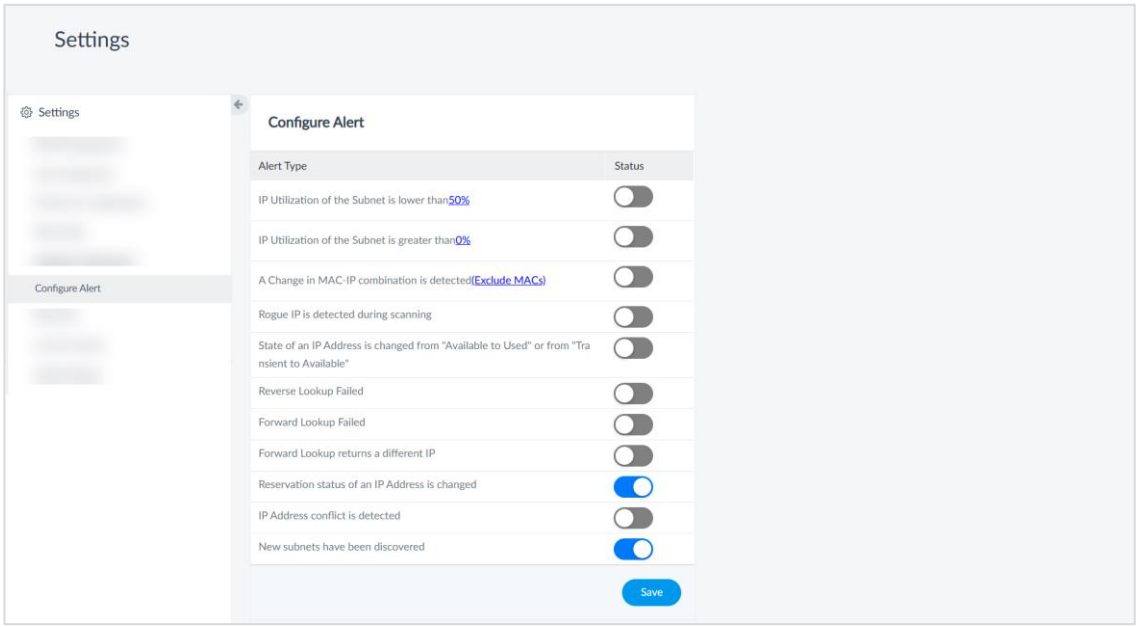


Fig 76: Configure Alert

The available alerts are:

- **IP Utilization of the Subnet is lower than %**: If the utilization of a subnet falls below the specified percentage, an email alert will be sent to the user configured in the Mail Server. You can specify the percentage by clicking the percentage link. **For example**, if you set the threshold to 70%, an alert will be triggered when utilization drops below 70%.

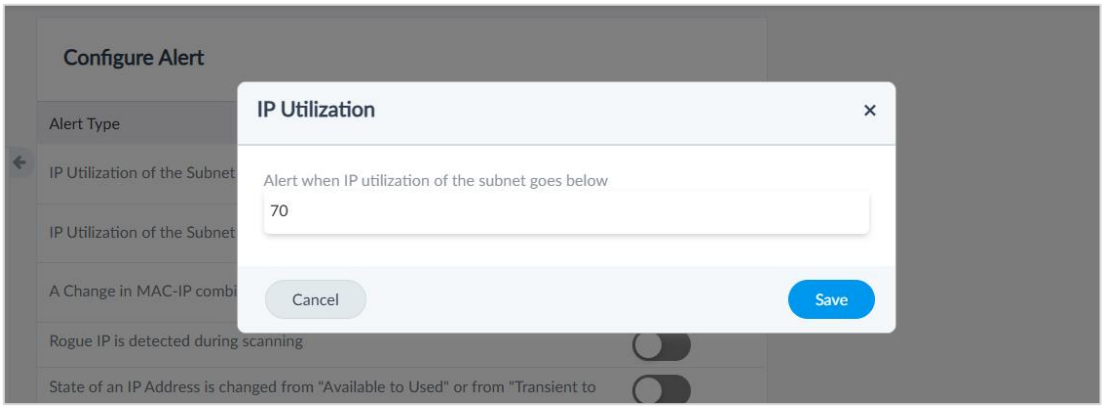


Fig 77: IP Utilization

- **IP Utilization of the Subnet is greater than %**: If the utilization of a subnet falls above the specified percentage, an email alert will be sent to the user configured in the Mail Server. You can specify the percentage by clicking the percentage link. **For example**, if you set the threshold to 70%, an alert will be triggered when utilization goes above 70%.

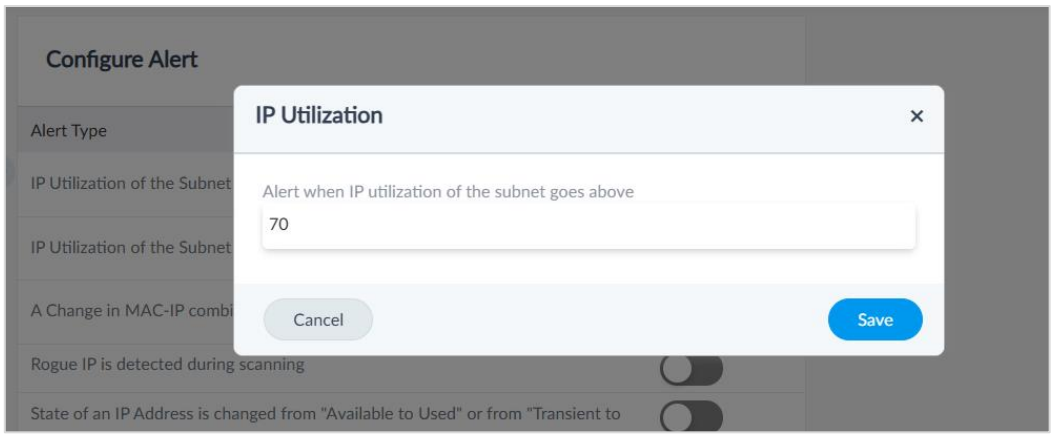


Fig 78: IP Utilization

- **A Change in MAC-IP combination is detected(Exclude MACs)**: Triggers an alert when a MAC-IP mapping changes, excluding any MAC addresses specified in the exclusion list. You can exclude the MAC addresses by clicking the **Exclude MACs** link.

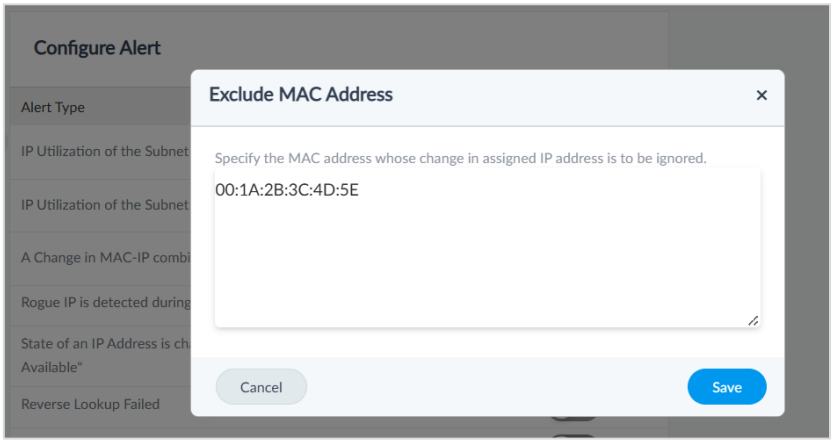


Fig 79: Exclude MAC Address

- **Rogue IP is detected during scanning**: Triggers an alert when an unknown or unauthorized IP is found during a scan.
- **State of an IP Address is changed from "Available to Used" or from "Transient to Available"**: Alerts when the status of an IP address changes.
- **Reverse Lookup Failed**: Notifies when the reverse DNS lookup for an IP address fails.
- **Forward Lookup Failed**: Notifies when the DNS name cannot be resolved to an IP address.
- **Forward Lookup returns a different IP**: Alerts when the DNS name resolves to a different IP than expected.
- **Reservation status of an IP Address is changed**: Triggers an alert when an IP address is reserved or its reservation is removed.
- **IP Address conflict is detected**: Notifies when two devices are found using the same IP address.
- **New subnets have been discovered**: Alerts when new subnets are added.

11.7. Discovery

Discovery in IPAM allows you to configure network gateways to identify and map subnets within your environment automatically. Once gateways are set up, IPAM scans and displays all discovered subnets, helping you maintain an accurate and up-to-date view of your IP infrastructure.

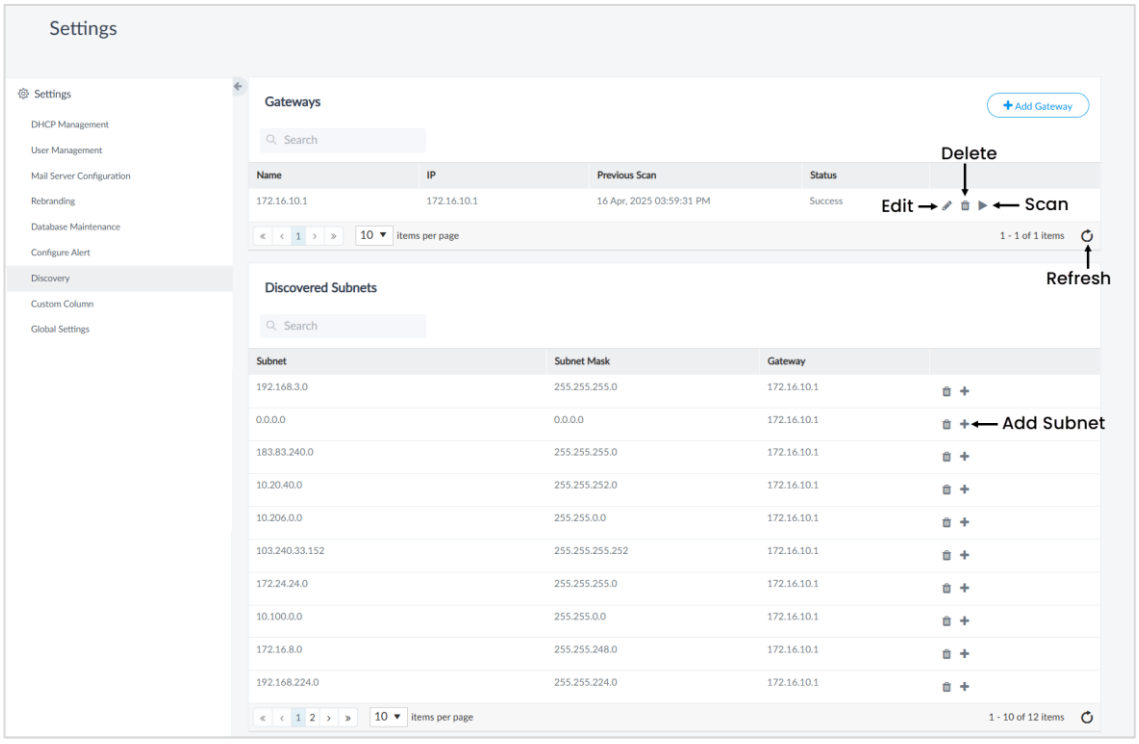


Fig 80: Discovery

Add Gateway

To add a gateway, follow the below steps:

1. Click the **+ Add Gateway** button, and the popup below will appear.

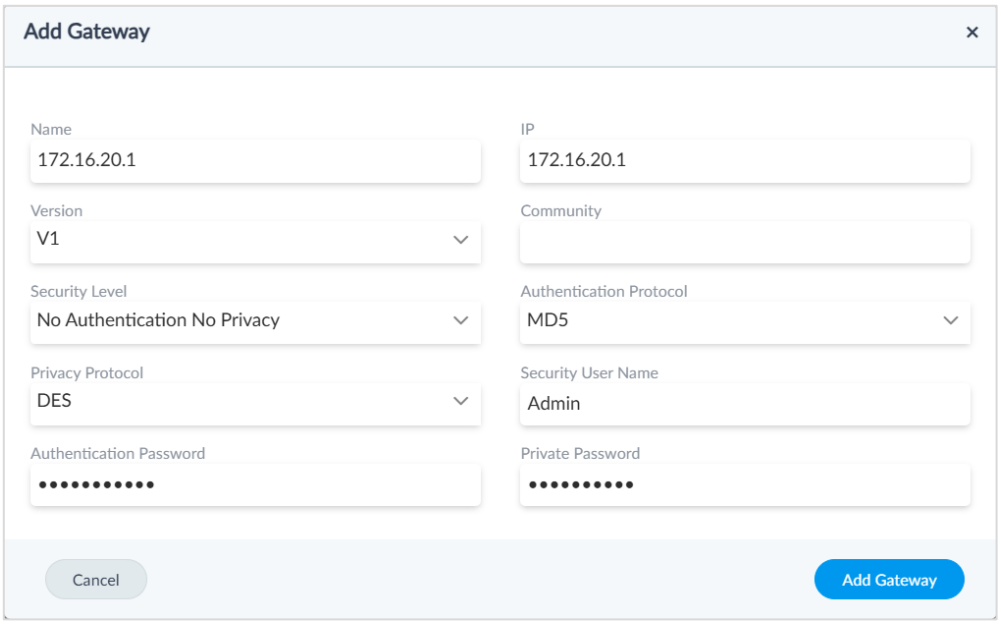


Fig 81: Add Gateway

2. Enter the below details:

- **Name**: Enter the name of the gateway.
- **IP**: Enter the gateway IP Address.
- **Version**: Select the version.
- **Community**: A shared string used as a password in SNMPv1/v2c to authenticate access to network devices. For example, public.
- **Security Level**: Defines the level of authentication and encryption used for SNMPv3 communication with the gateway. The options are:
  - **Authentication Privacy**: Uses authentication and encryption to ensure secure and private SNMP communication.
  - **No Authentication, No Privacy**: No authentication or encryption; communication is unsecured.
  - **Authentication No Privacy**: Verifies identity with authentication but does not encrypt the SNMP data.
- **Authentication Protocol**: Select the authentication protocol to be used for authentication. The options are:
  - **MD5:** An older hashing algorithm; less secure. It is used only for legacy device compatibility.
  - **SHA:** More secure than MD5 but still considered outdated. It is used only if newer SHA versions are not supported.
  - **SHA224:** Provides better security than SHA-1. It is used if the device supports it.

- **SHA256:** A widely recommended standard offering strong security; ideal for most environments.
- **SHA384:** Offers even stronger security than SHA256; preferred if supported and higher protection is needed.
- **SHA512:** The most secure option among the listed protocols; used when maximum security is required and supported.

- **Privacy Protocol**: Select the encryption algorithm used in SNMPv3 to secure data transmission and ensure confidentiality.
  - **DES:** A basic encryption method with limited security; use only for backward compatibility.
  - **3DES:** More secure than DES but slower and largely outdated; use if AES is not supported.
  - **AES:** Refers to standard AES encryption (typically 128-bit); reliable for general use.
  - **AES128:** 128-bit AES encryption; a strong and widely supported option for securing SNMP traffic.
  - **AES192:** 192-bit AES encryption offers stronger protection; use when higher security is needed.
  - **AES256:** 256-bit AES encryption; the most secure option, ideal for high-security environments.
- **Security User Name**: The SNMPv3 username is used to authenticate and communicate securely with the gateway. **Example**: snmpAdminUser
- **Authentication Password**: Used to verify the identity of the SNMPv3 user accessing the gateway. **Example**: AuthPass123!
- **Private Password**: Used to encrypt SNMPv3 communication for secure data transmission. **Example**: PrivKey456#

3. Once done, click **Add Gateway** to add it to the list. Then, click **Scan** ▶ to begin discovering subnets within the configured gateway. The scan status will change to **Running**, and upon completion, it will update to either **Success** or **Failed**, based on the outcome.
4. If successful, the associated subnets will appear in the Discovered Subnets below the Gateways section.
5. Once the subnets appear, you can add them to your network by clicking the **Add Subnet (+)** icon next to the required subnet. For more details on how to add Subnet, refer to the topic Add Subnet.

11.8. Custom Column

Custom Column allows users to add personalized data fields to the Subnet IP view, enabling better organization and tracking of IP-related information such as device owner, location, or asset tags—tailored to specific operational needs.

To add a custom column, follow the below steps:

1. Click the **+ Add Custom Column** button, and the following screen will appear.

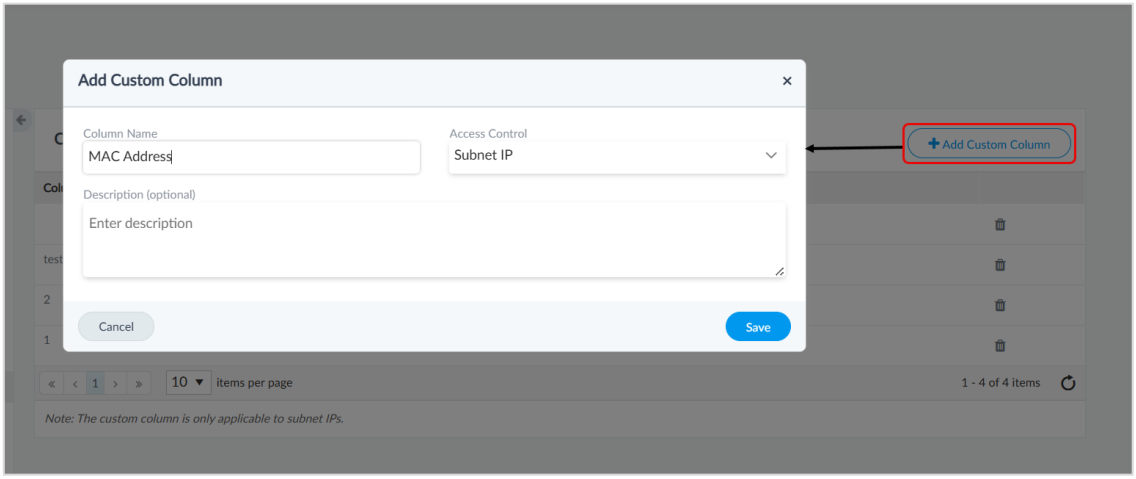


Fig 82: Add Custom Column

2. Enter the following details:
   - **Column Name**: Enter the column name.
   - **Access Control**: Select the access control.
   - **Description**: Enter a brief description of the column.
3. Once done, click **Save**. A maximum of 10 columns can be added. They will be displayed at the Subnet IP level.

Notes:

- Access to the Settings & Dashboard modules is required to configure these fields.
- The custom column is only applicable to subnet IPs.
- These columns are included in exported CSV/PDF reports but are not displayed in the on-screen report UI.

11.9. Global Settings

Global settings consist of the following configurations:

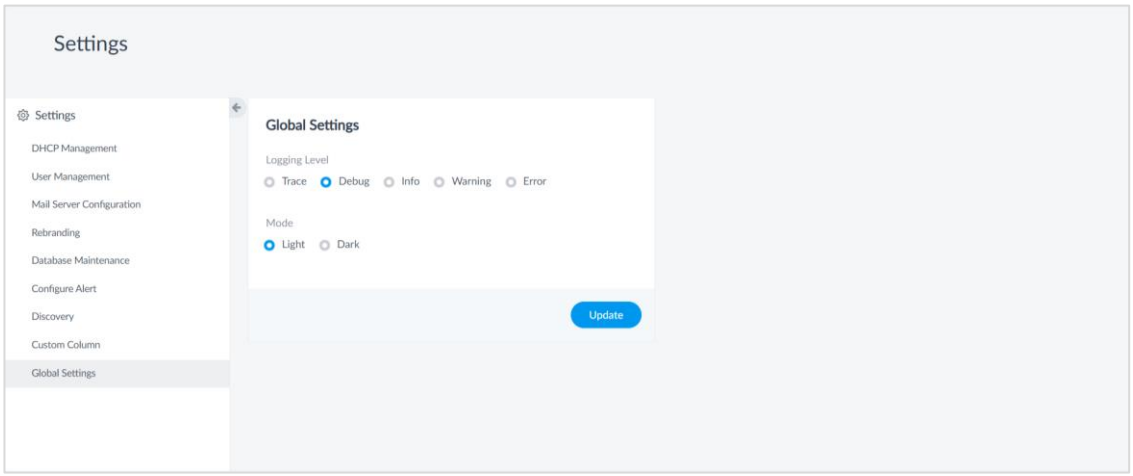


Fig 83: Global Settings Screen

Logging Level

You can set the specific logging level from global settings.

- **Trace** – It contains all detailed logs.
- **Debug** – It contains operations (Success/Failure).
- **Info** – It contains informational logs.
- **Warning** – It contains warning logs.
- **Error** – It contains all the error logs.

Mode

You can set the color theme of the application to either light or dark.

CONNECT WITH US

www.motadata.com

support@motadata.com