ADMINISTRATOR GUIDE

IP Address Manager

Version 2024.4

SOLARWINDS

Last Updated: Tuesday, October 15, 2024

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

Introduction

This is the Administrator Guide for IPAM IP Address Manager 2024.4. It forms part of the IPAM documentation set, and should be consulted after you have installed or upgraded IPAM and worked your way through the IPAM Getting Started Guide.

For instructions on installing and upgrading IPAM and other IPAM products, see the Solar Winds Installer.

Complete IPAM documentation in both online and PDF format can be found in the IPAM Documentation area of the Solar Winds Customer Success Center.

A video overview of IPAM can be found here: Manage Change and Avoid Costly Errors with SolarWinds IP Address Manager.

How IPAM works

IPAM provides integrated DNS, DHCP and IP address management, allowing you to monitor your entire IP address space from a single dashboard.

IPAM uses ICMP, SNMP and neighborhood scanning to collect details from the devices on your network, and uses this information to track and display IP address usage, and automatically mark IP addresses that are no longer in use. Additionally, WMI calls to DHCP and DNS servers are made to retrieve lease and scope details. You can make DHCP reservations and DNS entries for IP reservations all at once from a single screen. Data is stored for tracking and auditing purposes in the database. All statistics are accessible using the SolarWinds Web Console.

IPAM concepts and terminology

The following sections define networking concepts and terminology as used within IPAM. Some IPAM terms correspond specifically to status icons. See IPAM status icons for more information about the icons.

Available	All addresses in defined groups, subnets, and supernets are, by default, considered Available until they are otherwise assigned unless they are typically reserved, as in the case of the network address (*nnn.nnn.nnn*.0) and broadcast address (*nnn.nnn.nnn*.255). In IPAM, available IP addresses are indicated with a gray IP icon. See IPAM status icons for more information.

Classless Inter-Domain Routing (CIDR)

CIDR is the standard, scalable method for both designating and organizing IP addresses using variable length subnet masking to optimize packet routing efficiency over the Internet. In the CIDR standard, IP address blocks are represented using an IP address with a suffix, as in 214.100.48.00/20, where the suffix, /20, indicates the number of leading bits in the binary form of the IP address corresponding to the intended subnet.

The following examples show equivalent representations of the same subnet:

11010110.01100100.00111001.11010101 = 214.100.57.213/32

11010110.01100100.00111001.11010000 = 214.100.57.208/28

11010110.01100100.00111001.00000000 = 214.100.57.00/24

11010110.01100100.00110000.00000000 = 214.100.48.00/20

Using CIDR, network administrators have a great amount of flexibility in terms of defining the size of available IP address allocations. The basic formula for determining the size of a CIDR subnet is $s=2^{(n-32)}$, where S = the number of available IP addresses and n = the CIDR suffix. The following table displays the correlation between the CIDR suffix (/n) and the number of available IP addresses, or hosts, for multiple, different CIDR suffixes.

CIDR Suffix (/n)	Available IP Addresses (S)	CIDR Suffix (/n)	Available IP Addresses (S)
/31	2	/22	1022 = S - 2
/30	2 = S - 2	/20	4094 = S - 2
/28	14 = S - 2	/18	16382 = S - 2
/26	62 = S - 2	/16	65534 = S - 2
/24	254 = S - 2	/12	1048574 = S - 2

ⓘ In subnets defined to contain more than 2 IP addresses, typically the smallest address identifies the subnet to the rest of the network and the largest address is designated as the broadcast address for all addresses contained within the subnet.

	As a simple example case of CIDR notation with respect to subnets, both 214.100.50.20 and 214.100.61.45 are in the subnet 214.100.00.00/16 because they both share the same sixteen leading bits, represented by the decimal digits 214.100. These two IP addresses also exist in an even smaller subnet, 214.100.48.0/20, as revealed when the two addresses are expressed in binary, as follows, where the twenty leading bits are identical: 11010110.01100100.00110010.00000100 = 214.100.50.04 11010110.01100100.00111101.00101101 = 214.100.61.45 11010110.01100100.00110000.00000000 = 214.100.48.0/20
Group	In SolarWinds IPAM, groups serve as containers for the subnets, supernets, and even other groups you define to organize and manage your network. See IPAM groups for more information about creating and using groups in SolarWinds IPAM.
Reserved	In a subnet two IP addresses are reserved and cannot be assigned: • The network address • The broadcast address Other IP addresses can be reserved for special use in IPAM so they will not be assigned, either by an administrator or DHCP, to other devices. In SolarWinds IPAM, reserved IP addresses are indicated with a purple IP icon. See IPAM status icons for more information.
Static IP Address	A static IP address is an IP address assigned to a network device by an administrator. This is less efficient than using dynamic IP addresses as this permanently ties up the address even if it isn't being used. Certain types of servers, such as DHCP and DNS servers, always require static IP addresses.
Dynamic IP Address	A temporary IP address automatically assigned by a DHCP server to a network device when it is first detected. The IP address is released when the device is no longer detected.

Subnet

A subnet is any logical or physical subdivision of a network consisting of a collection of IP addresses for which some number of the leading address bits, commonly called an IP address routing prefix, are identical.

For example, as a simple case, both 214.100.50.20 and 214.100.61.45 are in the subnet 214.100.00.00/16, as they both share the same sixteen leading bits, represented by the decimal digits 214.100. Less obviously, these two IP addresses exist in an even smaller subnet, 214.100.48.00/20, as revealed when the two addresses are expressed in binary, as follows, where the twenty leading bits are identical:

214.100.50.04 = 11010110.01100100.00110010.00000100

214.100.61.45 = 11010110.01100100.00111101.00101101

11010110.01100100.00110000.00000000 = 214.100.48.00/20

Organizing your network using well-defined subnets can greatly increase the efficiency and minimize the bandwidth load on your network. At a basic level, assigning IP addresses to devices on your network in such a way that highly interactive devices reside within smaller or closer subnets reduces the amount of network traffic that must be routed over longer network distances. See Manage subnets in IPAM for more information about creating and managing subnets in SolarWinds IPAM.

Supernet

A supernet is an element of network organization consisting of contiguous CIDR blocks, or subnets. In networks with well-defined subnets, network administrators are able to consolidate and limit IP traffic with supernets to optimize routing efficiency across a network. As an example, given the following two subnets, 222.22.12.0/24 and 222.22.10.0/24, 222.22.0.0/20 is a supernet, as shown in the following expansions:

222.22.12.0/24 = 11011110.00010110.00001100.00000000

222.22.10.0/24 = 11011110.00010110.00001010.00000000

222.22.0.0/20= 11011110.00010110.00000000.00000000

Transient

IPAM uses the term Transient to describe IP addresses that are dynamically assigned to devices. IP addresses designated as Transient may be assigned to any of the following types of devices:

- Devices that power on and off regularly, such as laptops or some user workstations
- Devices that enter and exit the network frequently, such as laptops on a wireless network
- Any device on a DHCP-enabled network

> Transient scan intervals can be configured on a per subnet basis from the Edit Subnet window.

In IPAM, Transient IP addresses are indicated with a cyan colored IP icon. See IPAM status icons for more information.

Used

The Used label is provided to indicate any IP address that is currently assigned and not otherwise available. See IPAM status icons for more information.

Configure IPAM

This section includes the following topics:

Define system settings for IPAM

After you have installed and configured IPAM, you can edit the system settings to set variables to address your specific needs.

1. Click Settings > All Settings > IPAM Settings.
2. Click System Settings in the Settings section.

3. Edit settings as required.

General Settings	
Enable Duplicated Subnets	Enable this option to be able to create subnets that duplicate or overlap an existing subnet. If you have this setting enabled, IPAM will merge the status from multiple DHCP server scopes into one subnet (rather than having different subnets for each server's scope). For example, if an MSP has customers on duplicate internal addresses, you could create the duplicate space and give the subnet a different name.
Enable New User Interface	Check this box to use the new layout for the DHCP & DNS Management view. This is enabled by default.
Thresholds	
Critical Level	Define the Critical threshold for IP address space percentage usage in subnets and supernets. Subnets or supernets will be flagged with a red icon if at or above the critical threshold.
Warning Level	Define the Warning threshold for IP address space percentage usage in subnets and supernets. Subnets or supernets with a yellow icon if between the warning and critical levels.
Configuration Defaults	
Subnet scan enabled	When unchecked, the subnet scanning will be disabled in default.
Scan interval	The default interval between scans.
Automatically add IP addresses	Check to automatically add IP addresses when subnets are created.
CIDR	The default CIDR value.
Visual settings	
Tree sort by address	Disable will sort items in tree branch by 'Display Name' (rather than Address).
Tree max items	Maximum number of shown items per tree branch on Subnet Management page.

Network view items	The page size for Network view grid (Group view).
IP Address view items	The page size for IP Address view grid.
Personal settings	
Parent change notification message	Enable this option to display a notification message whenever you edit a parent account's specific custom roles.
ISC and BIND Settings	
No preserve timestamps	Enable this option if you do not want to preserve timestamps for configuration backup.

4. Click Save.

Configure subnet scan settings manually

IPAM uses SNMP and ICMP to scan and determine the status of your monitored network. You can select how IPAM automatically scans your network for changes.

1. Click Settings > All Settings > IPAM Settings > Manage Subnet Scan Settings.
2. Enter the transient period, or select Unlimited Duration.

   IPAM continuously scans all managed IP addresses on your network. If a device fails to respond to any SNMP or ICMP requests for the duration entered here, IPAM will change the status of the unresponsive IP address from Used to Available. Any associated custom attribute is overwritten. If Unlimited Duration is selected, unresponsive devices will retain the status of Used until manually updated.
3. ⓘ You can assign transient scan intervals for individual subnets using Edit Subnet Properties on the Manage Subnets and IP Addresses page.
4. ICMP is used by default to scan your network subnets for changes. To configure ICMP:
   a. Enter the number of pings per address.
   b. Enter the delay between pings, and the ping timeout, in milliseconds, for ICMP requests on your network.

5. To configure SNMP to scan your network subnets:
   a. Select Enable SNMP Scanning in the SNMP Scanning section.
   b. Select Enable SNMP neighbor scanning.
      Neighbor Scanning will attempt to retrieve the status of a device that is not responding to ICMP by scanning the ARP table of a neighbor router to determine what IP addresses are active.
   c. Enter the number of SNMP retries.
   d. Enter the SNMP Timeout, in milliseconds, for SNMP requests on your network.
6. Click Save.

ⓘ You can disable scanning on a per subnet basis. See Edit subnets for more information about editing individual subnet properties.

The IPAM Scan Job Status page

The Scan Job Status page displays all subnet scans currently in progress or scheduled for completion. Subnet scans are listed according to the Database Column property for each scanned subnet.

ⓘ The page also lists all DNS Zone Transfers.

View and edit subnet scans

ⓘ In addition to displaying subnet scan jobs, the Scan Job Status page also shows DNS Zone Transfers.

1. Click Settings > All Settings > IPAM Settings.
2. In the Subnet Scans section, click View scan job status. The Scan Job Status page provides the status of any jobs scheduled for scanning manually or automatically.

   The information for each subnet scan includes:

Status	Shows the time when the next scan of the corresponding subnet begins. If a scan is in progress, Status displays the time elapsed since the scan started.
Scan trigger	Shows whether automated or manually scheduled

Scan Type	This can be Subnet Scan or DNS Zone transfer.
Last Discovery	Shows the date and time when the corresponding subnet was last scanned.

3. The time to the next refresh is shown in the upper right of the screen,
4. To edit, click Edit at the end of a scan row.
   - If you click Edit for a Subnet scan, the Edit Subnet Properties window is displayed.
   - If you click Edit for a DNS Zone Transfer, the Edit a DNS zone page is displayed.
5. Make any required edits, and click Save.

Neighbor scanning in IPAM

Neighbor scanning attempts to retrieve the status of a device that is not responding to ICMP. It scans the ARP table of a neighbor router to determine what IP addresses are active.

> ⓘ Neighbor scanning is disabled by default, as it can increase router CPU usage, and therefore should only be enabled when needed.

1. Go to My Dashboards > IP Address Management > Manage Subnets & IP Addresses.
2. Select a subnet containing the device or devices that are not responding.
3. Click Edit.
4. Scroll to the bottom of the Edit Subnet Properties Window.
5. Uncheck the Disable Neighbor Scanning checkbox.

   Additional options are displayed.
6. Enter the Neighbor IP Address and select a Scan Interval.
7. Click Test to verify connection.
8. Click Save.

How Neighbor scanning works

IPAM first checks if the device is capable of SNMP and supports an ARP table.

- To check whether SNMP is available, IPAM uses these OIDs:

OidSysContact	"1.3.6.1.2.1.1.4.0" iso.org.dod.internet.mgmt.mib-2.system.sysContact.0

- To check whether the ARP table is available, it uses:

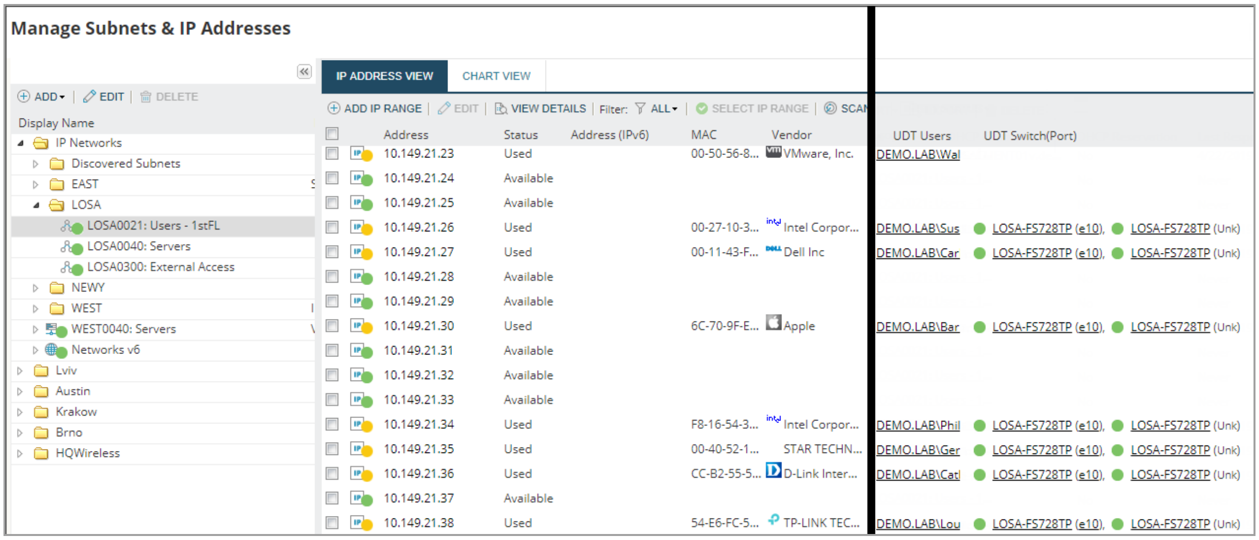
OidIPNetToMediaTable	"1.3.6.1.2.1.4.22" iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTable

The IPNetToMediaTable is pulled for client information. If the device supports this table, then IPAM can use this information.

Populate UDT User and Switch Ports in the IPAM IP Address View

Integration with SolarWinds User Device Tracker (UDT) adds User and Switch Ports columns to your IP Address view and provides end-to-end IP address to user-device mapping. IPAM detects if UDT is installed and automatically adds the columns.

1. Click My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Select a subnet.
   The UDT Users and UDT (Switch) Ports columns are the last two columns displayed in IP Address view. Scroll right if they are not displayed.



Manage Subnets & IP Addresses

Display Name
- IP Networks
  - Discovered Subnets
  - EAST
  - LOSA
    - LOSA0021: Users - 1stFL
    - LOSA0040: Servers
    - LOSA0300: External Access
  - NEWY
  - WEST
  - WEST0040: Servers
  - Networks v6
- Lviv
- Austin
- Krakow
- Brno
- HQWireless

Address	Status	Address (IPv6)	MAC	Vendor	UDT Users	UDT Switch(Port)
10.149.21.23	Used		00-50-56-8...	VMware, Inc.	DEMO.LAB\Wal	
10.149.21.24	Available					
10.149.21.25	Available					
10.149.21.26	Used		00-27-10-3...	Intel Corpor...	DEMO.LAB\Sus	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)
10.149.21.27	Used		00-11-43-F...	Dell Inc	DEMO.LAB\Car	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)
10.149.21.28	Available					
10.149.21.29	Available					
10.149.21.30	Used		6C-70-9F-E...	Apple	DEMO.LAB\Bar	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)
10.149.21.31	Available					
10.149.21.32	Available					
10.149.21.33	Available					
10.149.21.34	Used		F8-16-54-3...	Intel Corpor...	DEMO.LAB\Phil	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)
10.149.21.35	Used		00-40-52-1...	STAR TECHN...	DEMO.LAB\Ger	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)
10.149.21.36	Used		CC-B2-55-5...	D-Link Inter...	DEMO.LAB\Catl	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)
10.149.21.37	Available					
10.149.21.38	Used		54-E6-FC-5...	TP-LINK TEC...	DEMO.LAB\Lou	● LOSA-FS728TP (e10), ● LOSA-FS728TP (Unk)

3. If data for a device is being collected in UDT, these columns are populated, otherwise they will be empty.
    - Click on an entry in the UDT Users column to display the UDT Device Tracker User Details page for the user.
    - Clicking on the unbracketed part of entry in the UDT Switch (Port) column to display the NPM Node Details page for the associated node.
    - Clicking on an bracketed part of entry in the UDT Switch (Port) column, to display the UDT Device Tracker Port Details page for the ports on the node if direct and known.

See IP Address Conflicts for more information about using UDT and IPAM for troubleshooting issues.

Manage credentials

IPAM uses a variety of credentials to access information from different devices throughout your environment. The credentials must already be set up on the devices with the appropriate access level - for example for Windows DHCP servers it must be one of the three following groups: DHCP Users, DHCP Administrators or local Administrators.

Windows credentials

Windows Management Instrumentation (WMI) is are used throughout the IPAM (in products such as NPM, SAM and IPAM) to poll performance and management information from Windows-based network devices, applications, and components.

SNMP credentials

SNMP credentials are used to scan subnets and IP addresses. IPAM uses SNMP to poll device OIDs to obtain MAC addresses.

Scan credentials

DHCP and DNS server credentials can be set up either via the Add DHCP and Add DNS server pages when you are adding the servers, or created in advance using the Credentials for Scope scans page in IPAM Settings.

DHCP server credentials

IPAM scans the DHCP servers in your environment for scopes and subnets and therefore needs the appropriate credential for each DHCP server it scans.

DHCP Server Credentials	
Windows	For Windows computers running DHCP, a credential consists of user name and password.
CISCO	For Cisco devices running DHCP, a credential consists of user name and password, plus an optional enable level and enable mode password.
ASA	For Cisco Adaptive Security Appliance (ASA) devices running DHCP, a credential consists of user name and password, plus an optional enable level and enable mode password.
ISC	For Internet System Consortium (ISC) devices running DHCP, a credential consists of user name and password.
Infoblox	For the Infoblox environment, a credential consists of user name and password.

DNS server credentials

IPAM scans the DNS servers in your environment for DNS zones, settings and DNS zone transfers.

DNS Server Credentials	
Inherit credentials from SolarWinds node	This enables you to use the same credential as used for the parent node.
WMI	For Microsoft DNS servers, a WMI credential consists of user name and password.
BIND	For BIND servers, a credential consists of user name and password.
Infoblox	For the Infoblox environment, a credential consists of user name and password.

Add or edit SNMP credentials

You can store SNMP credentials to be used for scanning SNMP devices on your network. SolarWinds IPAM attempts SNMP communication using the stored credentials in the order provided.

1. Click Settings > All Settings > IPAM Settings > SNMP Credentials.
2. Either:
   - To add a new credential, click Add
   - To edit an existing credential, select the credential then click Edit.
3. Enter a display name for the credential.
4. Select the SNMP version of the credential. This can be SNMP v1, SNMP v2c, or SNMP v3.

   > ⓘ IPAM uses SNMPv2c by default.

   - For SNMP v1:
     a. Enter the SNMP Port and read only credential string. The defaults are 161 and "public".
   - For SNMP v2c:
     a. If you do not want IPAM to use SNMPv1 if an SNMPv2c request fails, check the Use SNMP v2 only checkbox.
     b. Enter the SNMP Port and read only credential string. The defaults are 161 and "public".
   - For SNMPv3:
     a. Enter the SNMP Port. The default is 161.
     b. Enter the User Name and Context string.
     c. Select the Authentication method, if used: this can be None, MD5 or SHA1
     d. Enter the Authentication password or key if used.
     e. Select the Privacy/Encryption method, if used: this can be None, DES56, AES128, AES192, or AES256.
     f. Enter the Privacy/Encryption password or key if used.
5. Click Save.

Add or edit Windows credentials

The Windows account specified within IPAM must be on the DHCP server and one of the three following groups: DHCP Users, DHCP Administrators or local Administrators. IPAM impersonates the specified account on the local computer to gain access. If the IPAM computer is not within the same Windows domain as the DHCP server, the IPAM computer must have the same identical account and password. All credentials are sent in clear text, so you should only update credentials through a browser while locally logged into the IPAM server or over an HTTPS connection.

ⓘ The Windows account must have the interactive log in rights enabled for IPAM to log in.

1. Click Settings > All Settings > IPAM Settings.
2. Under Manage Credentials, select Credentials for scope scans.
3. Either:
    - To add a new credential, click Add New and select Windows.
    - To edit an existing credential, select the credential then click Edit.
4. Enter a display name for this credential.
5. Enter a user name, and a password for this credential.
6. Click Save.

Add or edit Cisco and ASA credentials

IPAM uses CLI (command-line interface) commands and Telnet or SSH protocols to gather data from CISCO and ASA devices. Verify that your DHCP servers have configurable connection types (SSH or Telnet), ports, and a user name and password.

ⓘ If you change passwords on managed devices, ensure that you also change them in the IPAM credentials list.

1. Click Settings > All Settings > IPAM Settings > Credentials for Scope scans.
2. Either:
    - To add a new credential, click Add New and select CISCO or ASA.
    - To edit an existing credential, select the credential then click Edit.
3. Enter a name for this credential, the user name, and password.

    ⓘ The user name / password is for the user account you use to log in to the device through CLI to perform system configurations.

4. Select the Enable Level.

   > ⓘ The enable level must have privileges to execute configure terminal commands as well as to be able to configure IP SLA operations. For information on configuring network devices, please see your manufacturer's documentation.

5. Enter the Enable Password for this level.
6. Select the Protocol: Telnet or SSH.
7. Enter the Port.
8. Click Save.

Add BIND credentials

IPAM supports Linux-based BIND DNS Server monitoring and management. IPAM supports BIND version 8 and higher, although it is recommended you use BIND 9 as this supports commands for checking configuration syntax, which IPAM is able to use for configuration change validation during management operations. The BIND account specified within IPAM must be on the DHCP server and be DHCP users, DHCP administrators, or local administrators. If IPAM is not in the same BIND domain as the DHCP server, IPAM **must** have the identical account.

You can store BIND credentials for SolarWinds IPAM to access and scan your DHCP network devices. You can update credentials locally from the IPAM server or over an HTTPS connection.

> ⓘ The BIND account must have the interactive log in rights enabled for IPAM to log in.

1. Click Settings > All Settings > IPAM Settings > Credentials for Scope scans.
2. Either:
   - To add a new credential, click Add New and select Windows.
   - To edit an existing credential, select the credential then click Edit.
3. Enter a name for this credential, a user name, and a password for the credential.
4. Click Save.

Add or edit ISC credentials

IPAM supports ISC devices. You can store credentials to monitor your ISC Devices.

IPAM uses CLI (command-line interface) commands and Telnet or SSH protocols to gather data from ISC devices. Verify that your ISC DHCP servers have configurable connection types (SSH or Telnet), ports, and a user name and password.

ⓘ If you change passwords on managed devices, ensure that you also change them in the IPAM credentials list.

1. Click Settings > All Settings > IPAM Settings > Credentials for Scope scans.
2. Either:
    - To add a new credential, click Add New and select ISC.
    - To edit an existing credential, select the credential then click Edit.
3. Enter a name for this credential, the user name, and password.

    ⓘ The user name and password is the same user account you use to log in to the device through CLI to perform system configurations.

4. Select the Protocol: Telnet or SSH.
5. Enter the Port.
6. Click Save.

For a full list of ISC minimum requirements see Manage and monitor ISC DHCP servers and ISC DNS server settings in IPAM.

Infoblox credentials

IPAM 4.8 and later supports the monitoring of DNS, DHCP and IP information coming from your Infoblox environment.

IPAM uses a REST based Web API to gather data from the Infoblox environment.

ⓘ Since Infoblox monitoring is read-only certain IPAM operations are unavailable. For further information see Monitor the Infoblox environment.

1. Click Settings > All Settings > IPAM Settings > Credentials for Scope scans.
2. Either:
    - To add a new credential, click Add New and select Infoblox.
    - To edit an existing credential, select the credential then click Edit.
3. Enter a display name for the credential.
4. Enter a name for this credential, a user name, and a password for the credential.
5. Click Save.

User role delegation in IPAM

Role definitions enable you to restrict user access in IPAM and maintain security for your IP addresses without limiting the ability to delegate network management activities.

This section includes the following topics:

- Roles and privileges
- Add user accounts

Roles and privileges in IPAM

When you add a user account in IPAM, you assign the user a role. The role determines the user's privileges.

ⓘ If subnets are moved to create hierarchy changes, inherited roles are inherited from the new parent. Customized roles are not changed.

Role	Privileges
Administrator	The Administrator user role has read and write access, can initiate scans to all subnets, manage credentials, custom fields, and IPAM settings and has full access to DHCP management and DNS monitoring. Only administrators can perform certain actions, such as: • SNMP credentials management • Custom fields management • Subnet scan settings configuration • Directly configure custom roles in the Subnet Edit dialog
Power User	Power Users have the same privileges granted to Operators, with the addition of the following: • Drag-and-drop reorganization of network components in the Manage Subnets and IP Addresses view. • Supernet and group properties management, including the ability to edit supernet and group properties and custom fields on portions of the network made available by the Administrator. • Initiate scans.

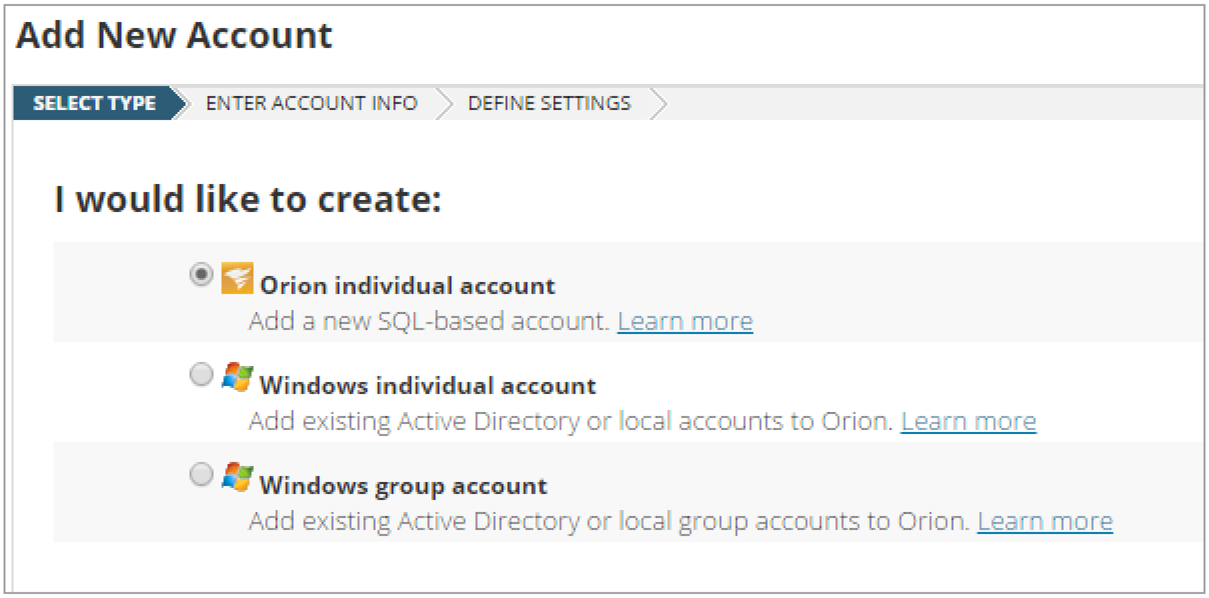
Operator	Operators have the same privileges granted to Read Only users with the addition of the following: • Addition and deletion of IP address ranges from portions of the network made available by the site administrator • Subnet status selection on the Manage Subnets & IP Addresses page • IP address property and custom field management, including the ability to edit IP address properties on portions of the network made available by the site administrator
Read Only	This role has read-only access to DHCP servers, scopes, leases, reservations and DNS servers, and zones. This role restricts all access, including access to all DHCP management and DNS monitoring, to the following: • All IPAM Web Console widgets, including search and Top XX widgets • All IP address and network component properties and custom fields on the Manage Subnets and IP Addresses page • The Chart view on the Manage Subnets & IP Addresses page
Custom	A Custom Role is customized on a per subnet basis and specifies which privileges a user has. You can also overwrite the inherited permissions on child objects. The child objects inherit the same permissions as the parent.

Add user accounts

You must add a user account for each person who needs to log in to IPAM. Each user is assigned a role, which determines the user's permissions.

1. Click Settings > All Settings > IPAM Settings > Manage Roles & Permissions.
2. Click Add New Account.

3. Choose an account type, and click Next.



Add New Account

SELECT TYPE › ENTER ACCOUNT INFO › DEFINE SETTINGS ›

I would like to create:

● Orion individual account
Add a new SQL-based account. Learn more

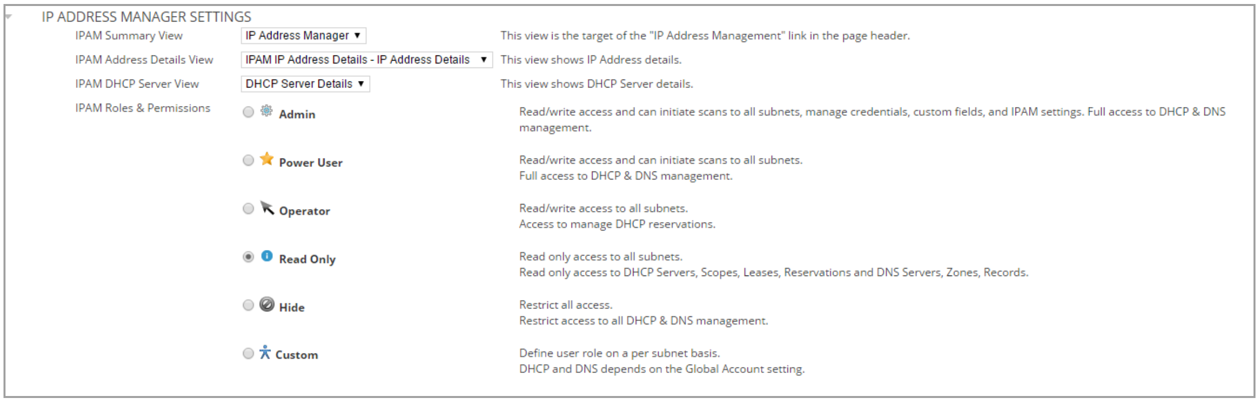
○ Windows individual account
Add existing Active Directory or local accounts to Orion. Learn more

○ Windows group account
Add existing Active Directory or local group accounts to Orion. Learn more

4. Enter the credentials, and click Next.
 For information on creating accounts for IPAM products, see Managing web accounts.

5. Define the general settings for SolarWinds Account Limitations and Menu Bar views.

6. Expand the IP Address Manager Settings near the bottom of the page.



IP ADDRESS MANAGER SETTINGS

IPAM Summary View: IP Address Manager ▾ — This view is the target of the "IP Address Management" link in the page header.

IPAM Address Details View: IPAM IP Address Details - IP Address Details ▾ — This view shows IP Address details.

IPAM DHCP Server View: DHCP Server Details ▾ — This view shows DHCP Server details.

IPAM Roles & Permissions

○ Admin — Read/write access and can initiate scans to all subnets, manage credentials, custom fields, and IPAM settings. Full access to DHCP & DNS management.

○ Power User — Read/write access and can initiate scans to all subnets.
Full access to DHCP & DNS management.

○ Operator — Read/write access to all subnets.
Access to manage DHCP reservations.

● Read Only — Read only access to all subnets.
Read only access to DHCP Servers, Scopes, Leases, Reservations and DNS Servers, Zones, Records.

○ Hide — Restrict all access.
Restrict access to all DHCP & DNS management.

○ Custom — Define user role on a per subnet basis.
DHCP and DNS depends on the Global Account setting.

7. Select the role and click Submit.

8. For information on creating a custom role, see Custom Roles.

Custom roles

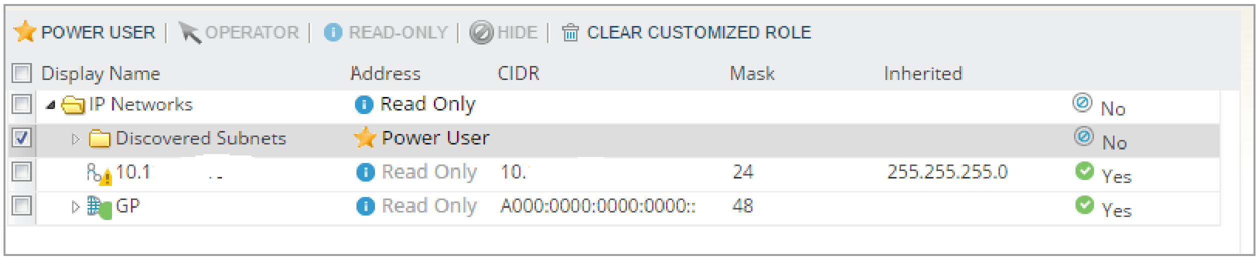
The following section covers how to create an IPAM custom role. These roles can be customized down to a per subnet basis.

The visibility of supernets and subnets depends on the role. The availability of operations is also affected by the role. You can overwrite the inherited permissions on child objects. The child objects inherit the same or higher permissions as the parent.

Define a custom role

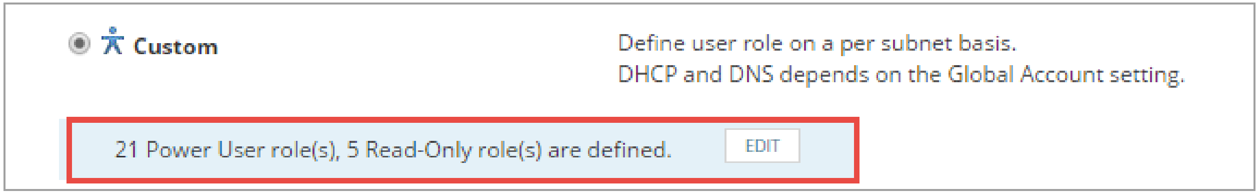
1. From the Role and Permissions selection box, select Custom, and click Edit.
2. Select a group or subnet, and choose a role. The Inherited column tells you if the role becomes inherited with other subnets.

> ⓘ For multiple selections, press the Ctrl key while selecting the group or subnet.



☐	Display Name	Address	CIDR	Mask	Inherited	
☐	IP Networks	Read Only				No
☑	Discovered Subnets	Power User				No
☐	10.1 . .	Read Only	10.	24	255.255.255.0	Yes
☐	GP	Read Only	A000:0000:0000:0000::	48		Yes

3. You can set permissions for particular subnets by selecting the subnet and then selecting a user role. The permission on the child object must be the same or higher than the parent object. After submitting, a message displays confirming the creation of the new role.

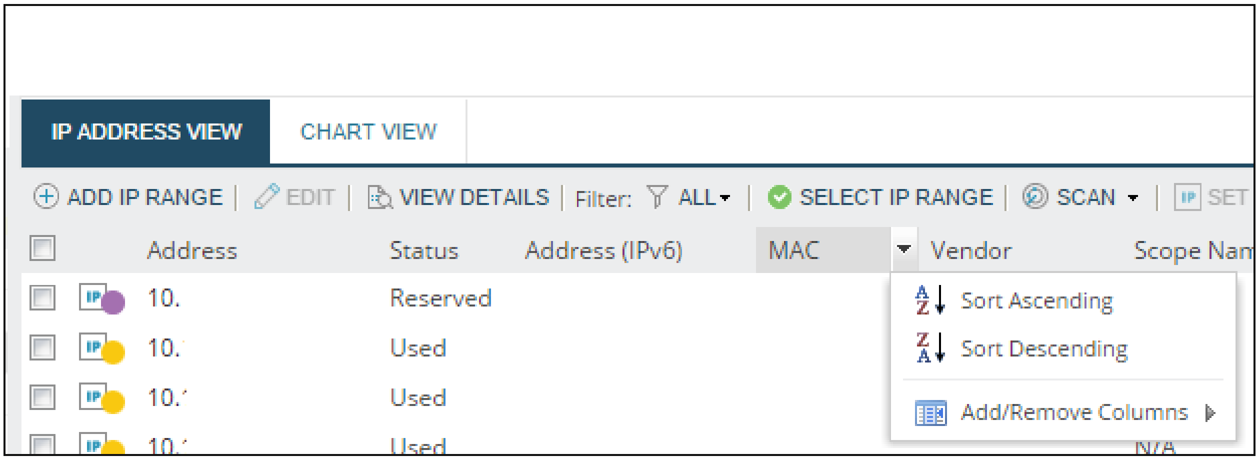


● Custom

Define user role on a per subnet basis.
DHCP and DNS depends on the Global Account setting.

21 Power User role(s), 5 Read-Only role(s) are defined.

To customize either the Network view or the IP Address view, click a column header and drag it to the preferred location. Your view personalization is saved immediately, and it is retained for the next time you use SolarWinds IPAM. From the menu, you can select which widgets to add, and resize the columns to fit your needs.



☐	Address	Status	Address (IPv6)	MAC	Vendor	Scope Nam
☐	10.	Reserved				
☐	10.	Used				
☐	10.'	Used				
☐	10.'	Used				N/A

Custom properties

Custom Properties are used throughout the IPAM, enabling you to set up user-defined fields such as country, building, room, asset tag, or serial number, that you can associate with monitored network objects from nodes to IP addresses.

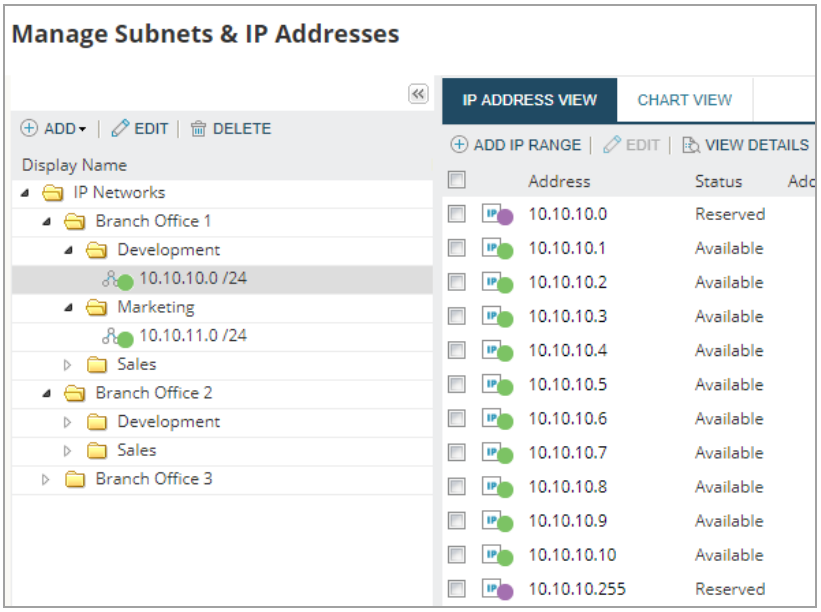
Any custom fields create in earlier versions of IPAM will be automatically converted to custom properties.

> ⓘ For more information on Custom properties, and its use throughout the IPAM, see Custom properties in the IPAM Administrator Guide.

IPAM groups

You can create groups in SolarWinds IPAM to help organize your network. The drag-and-drop user interface on the Manage Subnets & IP Addresses makes it easy to create groups containing any number of other groups, supernets, and subnets.

In the example below, a large network is spread over multiple offices, each with its own sales, marketing, and development departments.



Manage Subnets & IP Addresses

Display Name

- IP Networks
  - Branch Office 1
    - Development
      - 10.10.10.0 /24
    - Marketing
      - 10.10.11.0 /24
    - Sales
  - Branch Office 2
    - Development
    - Sales
  - Branch Office 3

□	Address	Status	Add
□	10.10.10.0	Reserved	
□	10.10.10.1	Available	
□	10.10.10.2	Available	
□	10.10.10.3	Available	
□	10.10.10.4	Available	
□	10.10.10.5	Available	
□	10.10.10.6	Available	
□	10.10.10.7	Available	
□	10.10.10.8	Available	
□	10.10.10.9	Available	
□	10.10.10.10	Available	
□	10.10.10.255	Reserved	

Each branch office unit has its own assigned IP addresses or subnet. You can group all the various network components related to each department of each branch office into its own group.

Create groups

1. Click My Dashboards > IP Address Manager > Manage Subnets & IP Addresses.
2. Click Add > Group.
3. Enter a name for the group.
4. (Optional) Add a description and custom properties for the group.
5. Click Save.

You can now drag and drop other groups, subnets, and supernets into your group to organize your network.

> Groups can be edited by selecting the group in step 2 and clicking Edit.

Add Additional Polling Engines to IPAM

IPAM supports Additional Polling Engines (APEs). If you have a large number of subnets, Additional Polling Engines can reduce the time it takes to scan your network. This topic documents how to install Additional Polling Engines.

> ⓘ To learn how to change the polling engine assigned to scan a specific subnet, as well as how to look up the polling engine monitoring a DNS server or DHCP server instance that IPAM manages, see Display or change polling engine assignments in IPAM.

Step 1: Download the Poller installer

1. Open the SolarWinds Web Console and choose Settings > All Settings.

   The Main Settings & Administration page opens.
2. Scroll down to the Details section.
3. Click Polling Engines.

   The Polling Engines page opens.
4. Click the DOWNLOAD INSTALLER NOW link in the top-right corner, and save the `SolarWinds-Orion-Installer.exe` file to your system.

Step 2: Run the Additional Polling Engine installer

1. Double-click the `SolarWinds-Orion-Installer.exe` file.

   The installer opens.

2. Use the wizard to complete the installation.

Display or change polling engine assignments in IPAM

This section documents how to change the polling engine assigned to scan a specific subnet, as well as how to look up the polling engine monitoring a DNS server or DHCP server instance that IPAM manages. If you have a large number of subnets, Additional Polling Engines (APEs) can reduce the time it takes to scan your network. Use the SolarWinds Web Console to assign a polling engine to scan individual subnets.

> ⓘ To learn how to install Additional Polling Engines, see Add Additional Polling Engines to IPAM.

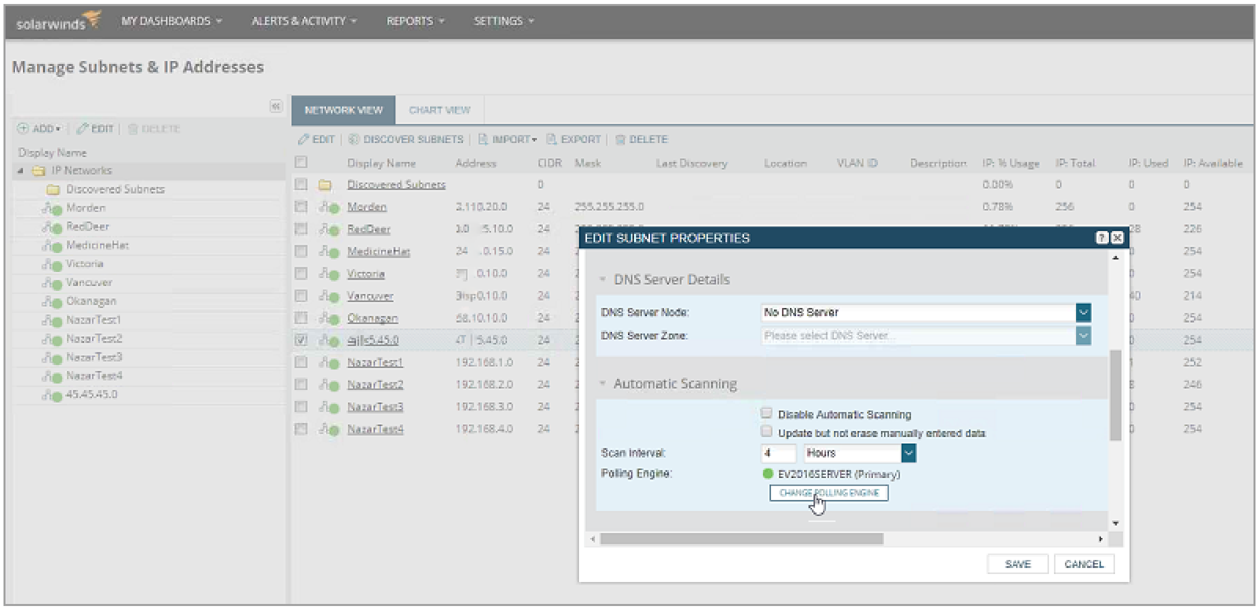
Complete these steps to change the polling engine assigned to automatic scanning.

1. Open the SolarWinds Web Console and choose My Dashboards > IP Addresses > Manage Subnets & IP Addresses.

   The Manage Subnets & IP Addresses page opens.

2. Select a subnet.
3. Click Edit.

   The Edit Subnet Properties dialog box opens. The Polling Engine is displayed.



EDIT SUBNET PROPERTIES

DNS Server Details

DNS Server Node: No DNS Server

DNS Server Zone: Please select DNS Server...

Automatic Scanning

□ Disable Automatic Scanning

□ Update but not erase manually entered data

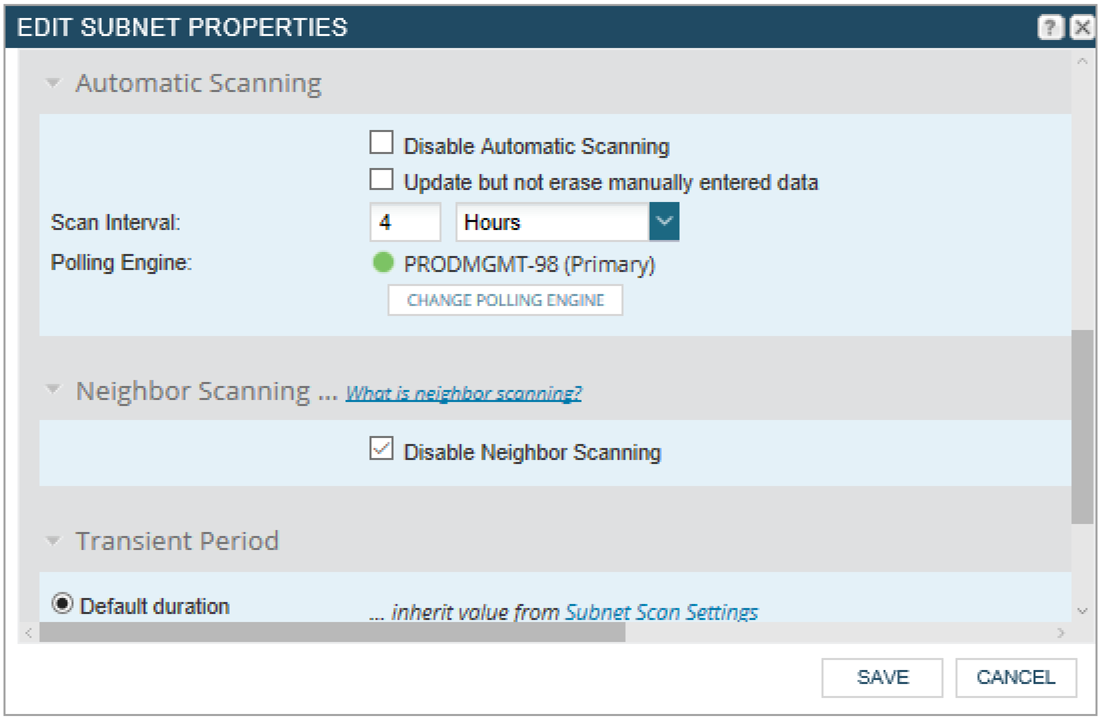
Scan Interval: 4 Hours

Polling Engine: ● EV2016SERVER (Primary)

CHANGE POLLING ENGINE

SAVE CANCEL

4. Scroll down to the Automatic Scanning section.



EDIT SUBNET PROPERTIES

Automatic Scanning

□ Disable Automatic Scanning

□ Update but not erase manually entered data

Scan Interval: 4 Hours

Polling Engine: ● PRODMGMT-98 (Primary)

CHANGE POLLING ENGINE

Neighbor Scanning ... What is neighbor scanning?

☑ Disable Neighbor Scanning

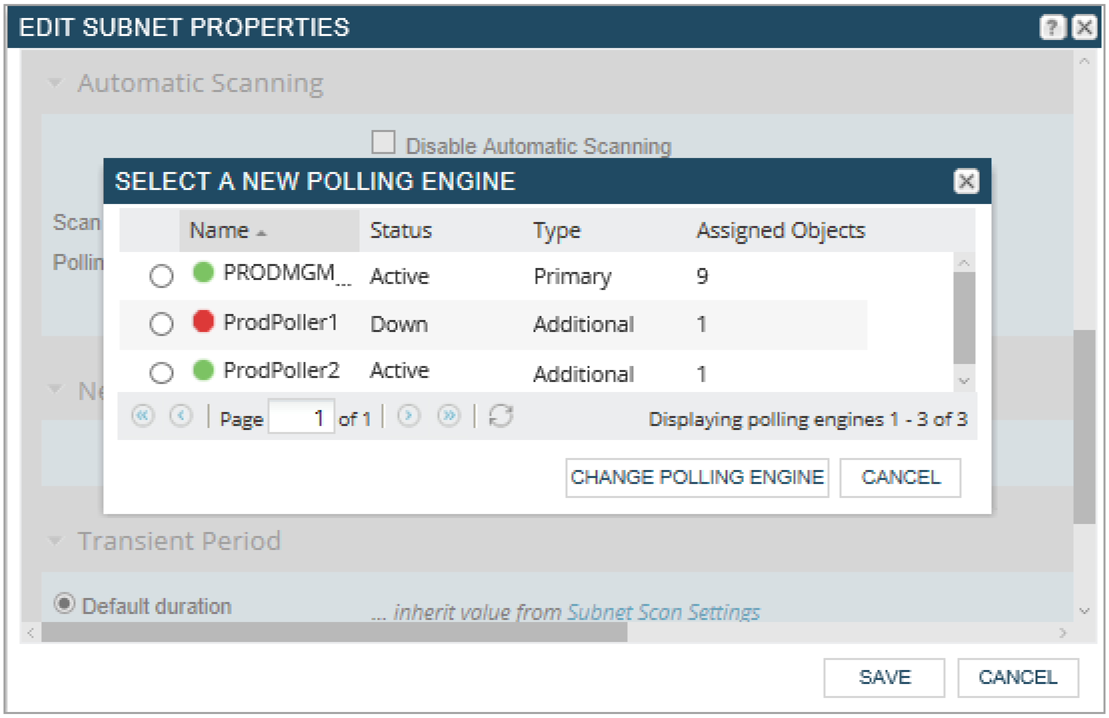
Transient Period

● Default duration ... inherit value from Subnet Scan Settings

SAVE CANCEL

5. Click Change Polling Engine.

   The Select a New Polling Engine dialog box opens.



EDIT SUBNET PROPERTIES

Automatic Scanning

☐ Disable Automatic Scanning

Scan

Pollin

SELECT A NEW POLLING ENGINE

	Name ▲	Status	Type	Assigned Objects
○	● PRODMGM...	Active	Primary	9
○	● ProdPoller1	Down	Additional	1
○	● ProdPoller2	Active	Additional	1

Page 1 of 1 | Displaying polling engines 1 - 3 of 3

CHANGE POLLING ENGINE | CANCEL

Ne

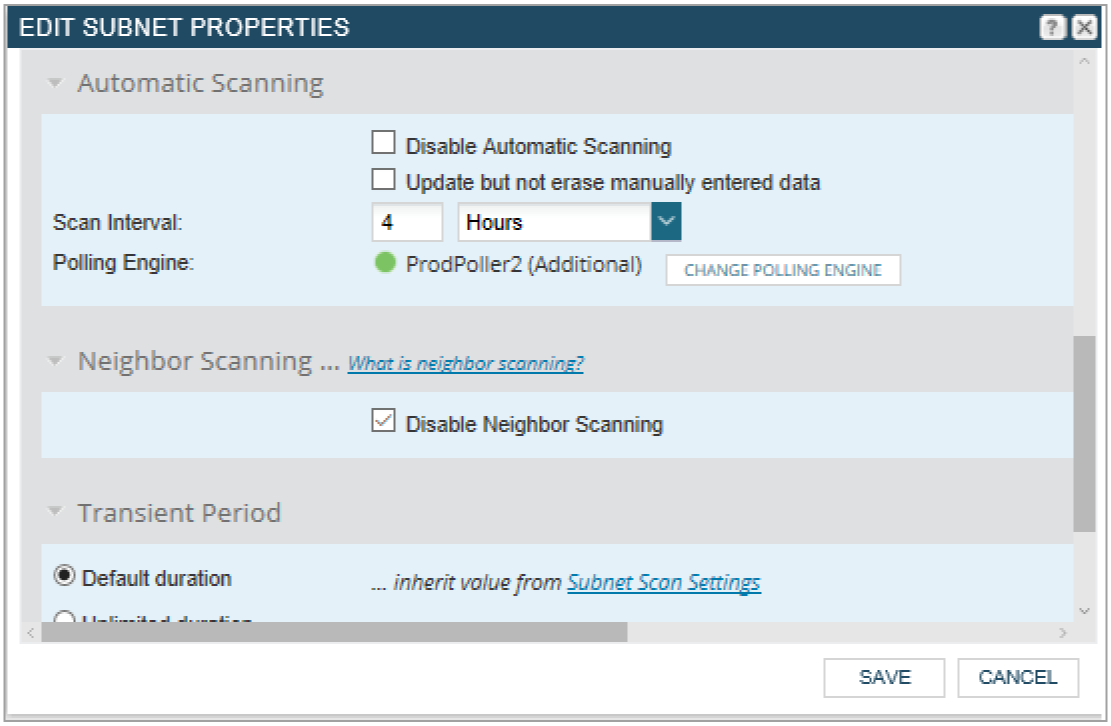
Transient Period

● Default duration ... *inherit value from Subnet Scan Settings*

SAVE | CANCEL

6. Select a polling engine and then click Change Polling Engine.

   The new polling engine is listed in the Automatic Scanning section.



EDIT SUBNET PROPERTIES

Automatic Scanning

☐ Disable Automatic Scanning

☐ Update but not erase manually entered data

Scan Interval: 4 Hours

Polling Engine: ● ProdPoller2 (Additional) CHANGE POLLING ENGINE

Neighbor Scanning ... *What is neighbor scanning?*

☑ Disable Neighbor Scanning

Transient Period

● Default duration ... *inherit value from Subnet Scan Settings*

○ Unlimited duration

SAVE | CANCEL

7. Click Save to close the Edit Subnet Properties dialog box.

Add IP addresses to IPAM

IP addresses need to be added to IPAM before they can be monitored. The following options are available for adding IP addresses to IPAM:

A range of IP addresses can be added to any defined subnet. This is usually done when you want to monitor specific addresses within a large subnet. For smaller subnets containing 4096 or fewer IP addresses (/21, or 255.255.248.0 and higher mask), SolarWinds IPAM automatically monitors all included IP addresses.

> ⓘ IPAM automatically **monitors** all IP addresses in subnets defined with 4096 IP addresses (/21 or 255.255.248.0 mask) or fewer. You can **manage** IP addresses in larger subnets with these ranges.

To add IP addresses for monitoring, add a parent subnet into any of the following:

- An existing group
- A supernet
- A subnet to a group that SolarWinds IPAM is monitoring

See Create subnets for more information about adding subnets.

Use the Subnet Allocation wizard to directly define subnets and allocate included IP addresses.

You can also add IPv6 sites and addresses for planning purposes. See IPv6 Addresses for more information.

Discover devices using Active Directory domain controllers

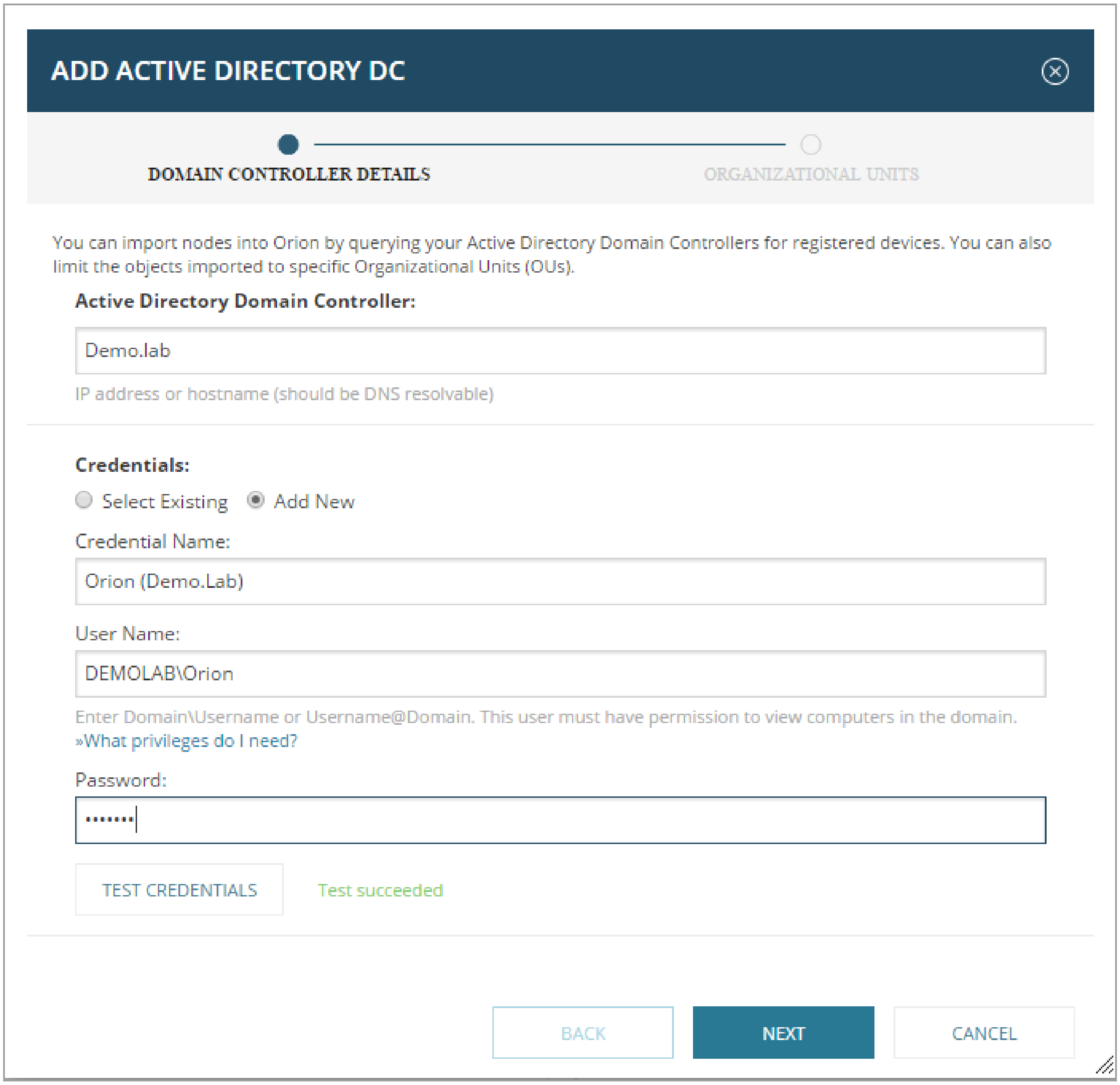
You can query your Active Directory Domain Controller to add nodes quickly and efficiently. Your SolarWinds server can use the devices specified in Active Directory instead of scanning every IP address in the subnet.

1. Navigate to Settings > Network Discovery.

   > ⓘ If a discovery has already been run, the Network Sonar Discovery page is displayed. Click Add New Discovery.

2. Click Start.
3. On the Network Sonar Wizard - Network Selection, click Add Active Directory Controller to query.

   The Add Active Directory DC pop-up is displayed.



ADD ACTIVE DIRECTORY DC

You can import nodes into Orion by querying your Active Directory Domain Controllers for registered devices. You can also limit the objects imported to specific Organizational Units (OUs).

Active Directory Domain Controller: Demo.lab

IP address or hostname (should be DNS resolvable)

Credentials: ○ Select Existing ● Add New

Credential Name: Orion (Demo.Lab)

User Name: DEMOLAB\Orion

Enter Domain\Username or Username@Domain. This user must have permission to view computers in the domain.
»What privileges do I need?

Password: •••••••

TEST CREDENTIALS Test succeeded

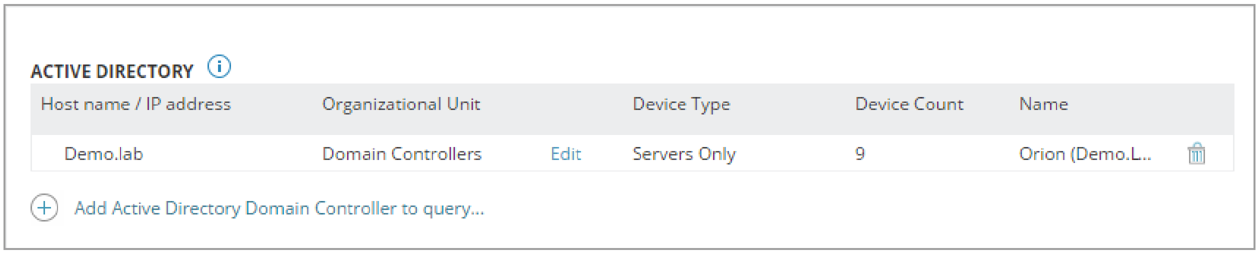
4. Enter an IP address or host name in the Active Directory Domain Controller field.

5. Use an existing credential or select Add New credential and enter the credential name, user name, and password.
6. Click Test Credentials. If valid, click Next.
7. Select the organizational units (OUs) you want to scan for nodes, and click Finish.

   > By default, all OUs are selected, but only servers will be added. Add workstations by clearing the Import servers only check box below the OUs.

8. On the Network Sonar Wizard - Network tab, click Next.

   In this example, nine devices were found.



ACTIVE DIRECTORY

Host name / IP address	Organizational Unit		Device Type	Device Count	Name	
Demo.lab	Domain Controllers	Edit	Servers Only	9	Orion (Demo.L...	🗑

⊕ Add Active Directory Domain Controller to query...

9. Continue the Network Discovery by clicking Next to each tab until the Discovery Scheduling tab is displayed.
10. Click Discover.

    The discovery is run.

11. Click Next to each tab to select the required devices, ports and volumes to import.

Add discovered devices to SolarWinds IPAM

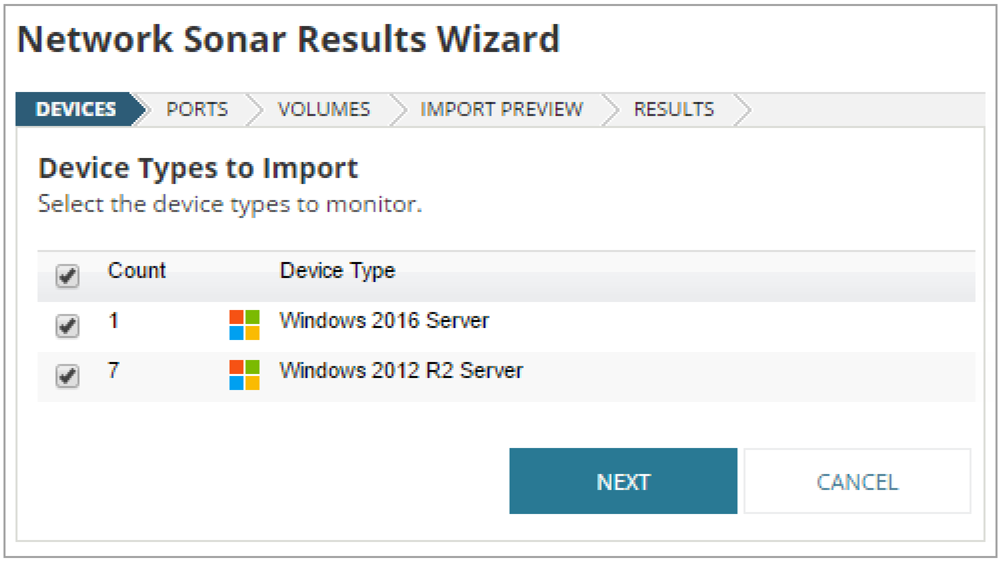
After the wizard has discovered the devices on your network, the Results screen opens, enabling you to import network elements into the SolarWinds database. Discovered elements do not count against your license count; only elements that are imported into the SolarWinds database count against your license.

When you manually run discovery, the system automatically selects all network elements to be monitored. You must clear the check boxes for elements you do not want monitored.

> If you are discovering your network for the first time, SolarWinds recommends that you start by monitoring a small number of devices.

After discovering your network, use the wizard to select the devices you want to monitor.

1. Ensure that only the device types you want to monitor are selected, and click Next.



Device Types to Import

Select the device types to monitor.

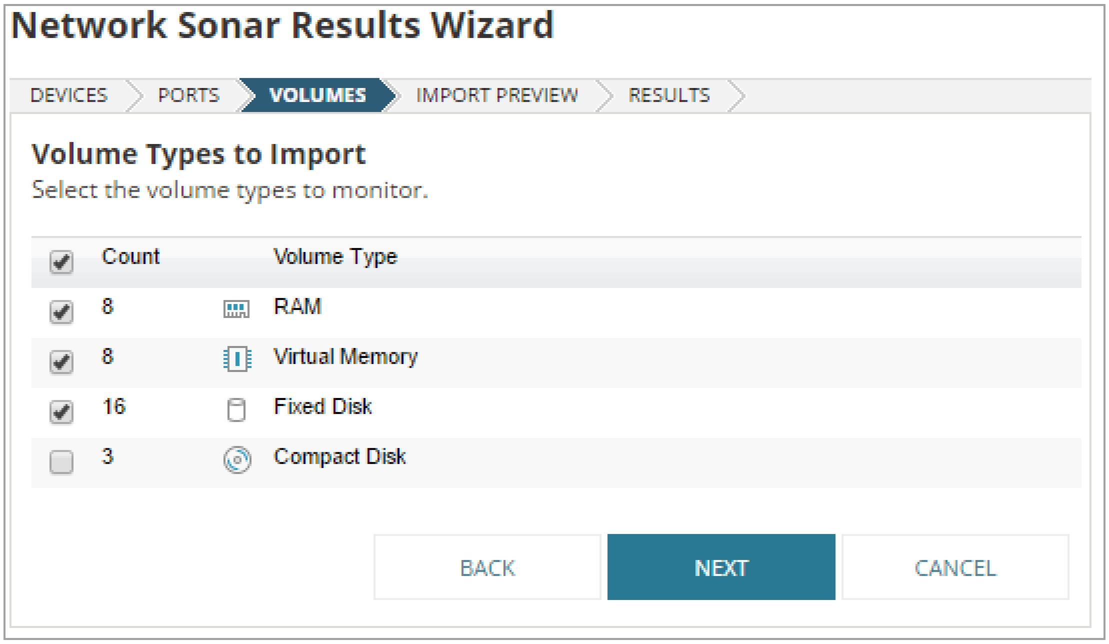
☑	Count	Device Type
☑	1	Windows 2016 Server
☑	7	Windows 2012 R2 Server

2. If the Ports tab is displayed, select the ports to monitor, and click Next.

   ⓘ The Ports tab is only available if you have User Device Tracker (UDT) installed.

3. Ensure the volume types you want to monitor are selected, and click Next.

   SolarWinds recommends that you do not monitor compact disks or removable disks.

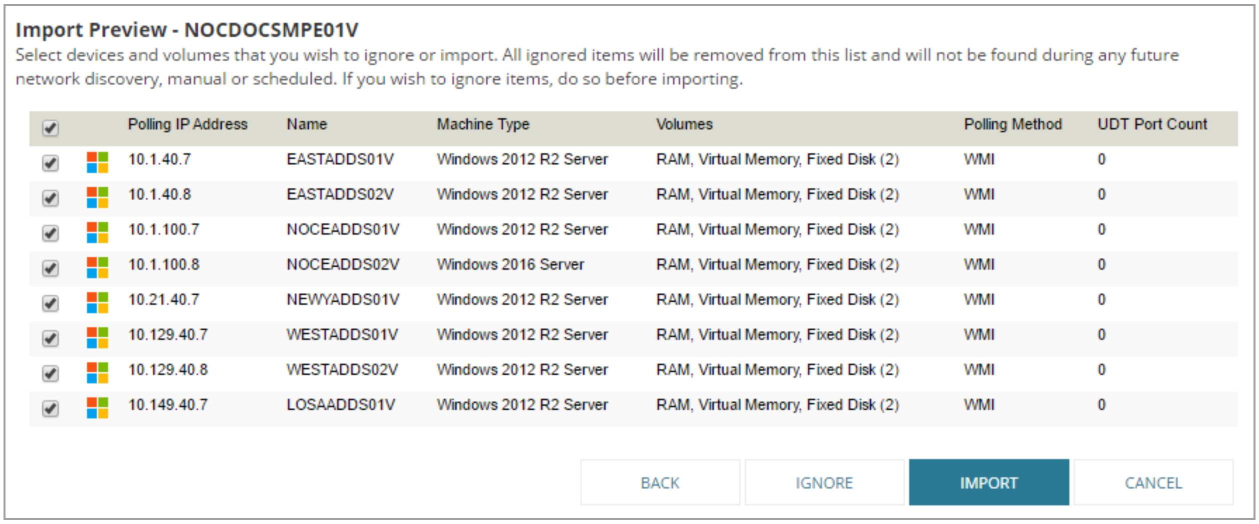


Volume Types to Import

Select the volume types to monitor.

☑	Count	Volume Type
☑	8	RAM
☑	8	Virtual Memory
☑	16	Fixed Disk
☐	3	Compact Disk

4. Review the list of elements to be imported, and click Import.



Import Preview - NOCDOCSMPE01V

Select devices and volumes that you wish to ignore or import. All ignored items will be removed from this list and will not be found during any future network discovery, manual or scheduled. If you wish to ignore items, do so before importing.

☑	Polling IP Address	Name	Machine Type	Volumes	Polling Method	UDT Port Count
☑	10.1.40.7	EASTADDS01V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.1.40.8	EASTADDS02V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.1.100.7	NOCEADDS01V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.1.100.8	NOCEADDS02V	Windows 2016 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.21.40.7	NEWYADDS01V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.129.40.7	WESTADDS01V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.129.40.8	WESTADDS02V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0
☑	10.149.40.7	LOSAADDS01V	Windows 2012 R2 Server	RAM, Virtual Memory, Fixed Disk (2)	WMI	0

5. When the import completes, on the Results panel, click Finish.

6. Click My Dashboards > IPAM Summary to begin exploring your network.

Import IP addresses

IPAM provides two methods to easily import IP addresses and subnet data into your network, either by importing from spreadsheets as described in this topic, or bulk adding by entering Subnet/CIDR prefixes.

With the IPAM 2019.4 and newer releases, you can import and export IPv6 addresses.

For exporting IP Addresses, see Export Subnets.

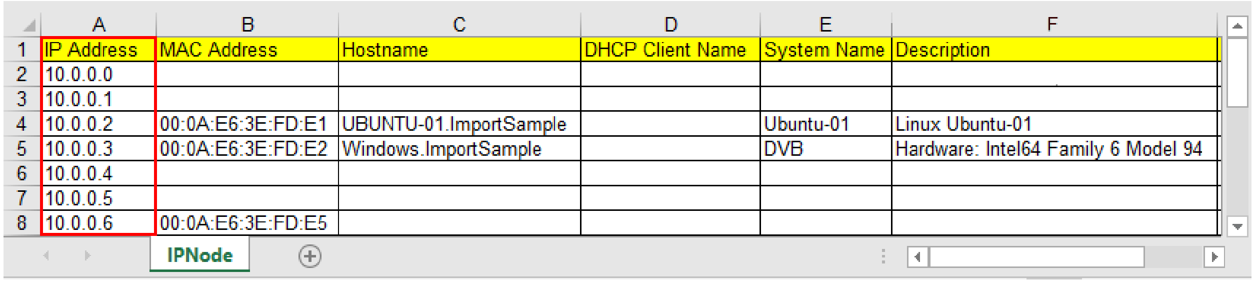
Import from spreadsheet

The IPAM Import wizard enables you to easily import IP addresses, and subnet and network data that is held on spreadsheets. You can import IP4 and IP6 groups, supernets, and IPV6 global prefixes, and the hierarchy structure of your network.

Imported data respects user delegation permissions.

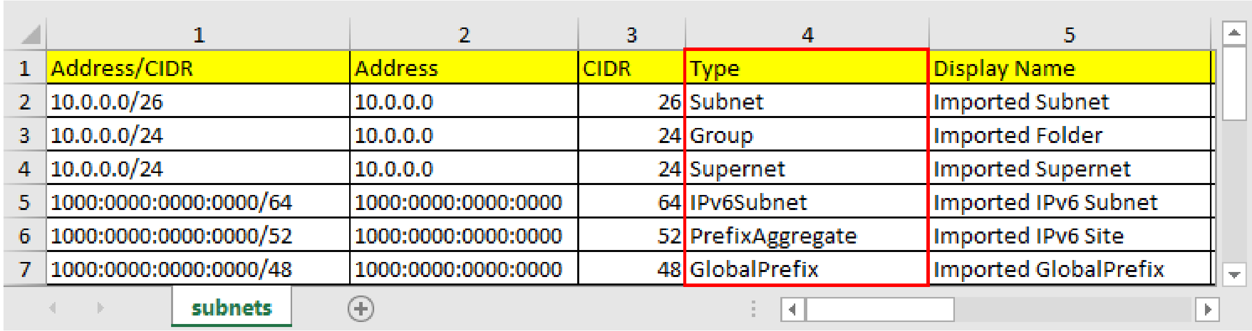
All imported spreadsheets require a header row with unique column names. These do not need to match the IPAM field names as you can associate each column with the field into which it is imported. Any columns that do not have corresponding fields in IPAM can be added as custom fields.

A subnet spreadsheet contains an IP address on each row. Only the IP Address is mandatory.



	A	B	C	D	E	F
1	IP Address	MAC Address	Hostname	DHCP Client Name	System Name	Description
2	10.0.0.0					
3	10.0.0.1					
4	10.0.0.2	00:0A:E6:3E:FD:E1	UBUNTU-01.ImportSample		Ubuntu-01	Linux Ubuntu-01
5	10.0.0.3	00:0A:E6:3E:FD:E2	Windows.ImportSample		DVB	Hardware: Intel64 Family 6 Model 94
6	10.0.0.4					
7	10.0.0.5					
8	10.0.0.6	00:0A:E6:3E:FD:E5				

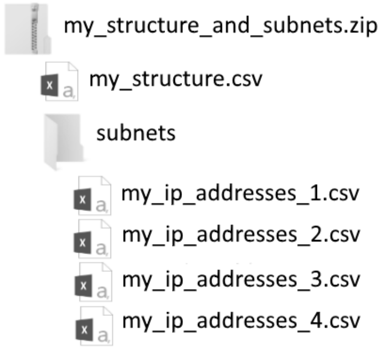
For a structure spreadsheet, only the Type of each object needs to be provided. This can be Group, Supernet, Subnet, IPv6Subnet, GlobalPrefix, PrefixAggregate, etc.



	1	2	3	4	5
1	Address/CIDR	Address	CIDR	Type	Display Name
2	10.0.0.0/26	10.0.0.0	26	Subnet	Imported Subnet
3	10.0.0.0/24	10.0.0.0	24	Group	Imported Folder
4	10.0.0.0/24	10.0.0.0	24	Supernet	Imported Supernet
5	1000:0000:0000:0000/64	1000:0000:0000:0000	64	IPv6Subnet	Imported IPv6 Subnet
6	1000:0000:0000:0000/52	1000:0000:0000:0000	52	PrefixAggregate	Imported IPv6 Site
7	1000:0000:0000:0000/48	1000:0000:0000:0000	48	GlobalPrefix	Imported GlobalPrefix

Subnet or Structure spreadsheets can be imported as individual .csv, .xls, or .xlsx files.

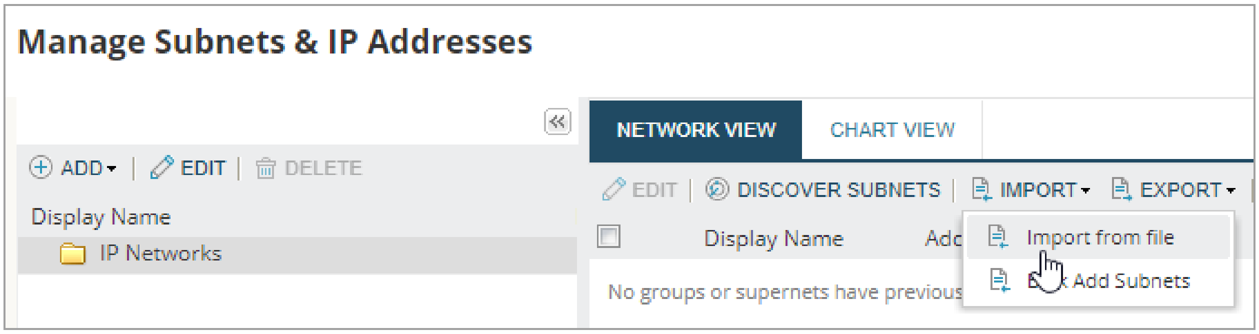
To import a structure spreadsheet with associated subnet spreadsheets, save the subnet spreadsheets in a subdirectory called Subnets and create a zip file containing all the files as shown below.



my_structure_and_subnets.zip
my_structure.csv
subnets
my_ip_addresses_1.csv
my_ip_addresses_2.csv
my_ip_addresses_3.csv
my_ip_addresses_4.csv

You can choose whether to import data into new and existing IP subnets, preserving the hierarchies in the structure spreadsheet, or into an imported subnet folder with a flat file structure to be organized later.

1. Navigate to My Dashboards > IP Addresses > Manage Subnets & IP Addresses.



No groups or supernets have previous

2. Click Import > Import from file.

   The Preparing to import a spreadsheet page is displayed. This page enables you to download example spreadsheets that can help you create your own spreadsheets.

3. Click Next to proceed.

   > ⓘ You can avoid showing the Preparing to import a spreadsheet page every time by checking the Don't show this again box.

4. Click Browse.
5. Navigate to the required file, and click Open.
6. Select the type of import, and click Next:

   IP Addresses: Select this if you have a single spreadsheet list of IP addresses,

   Structure only: Select to import a spread containing the structure for your IP addresses

   Structure and IP Addresses: Select of you have zipped the structure spreadsheet with associated IP address spreadsheets in a sub-directory (see above).

Import IP Addresses

1. The IP Address column matching page is displayed, showing the IPAM IP address fields and what the wizard has determined to be the corresponding columns in the spreadsheet. If these are not correct or you do not want to import anything for a field, use the drop-down menu to select an alternative field.

   Select [Do not import] for fields that do not have a corresponding column in the spreadsheet.

   The only mandatory field for this import is the IP Address.

2. Click Next.

3. The Subnet Column matching page is displayed, showing the IPAM subnet fields and what the wizard has determined to be the corresponding columns in the spreadsheet. If these are not correct, or you do not want to import anything for a field, use the drop-down menu to select an alternative field.

   Select [Do not import] for fields that do not have a corresponding column in the spreadsheet.

   There are no mandatory fields for subnet information.

4. Select the option for where you want the imported subnets to go, and click Next:

   - IPAM will automatically create subnet hierarchy in selected location based on import
   - IPAM will import subnets into the "Imported Subnet" folder (flat file structure)

5. If your spreadsheet contains additional columns to those IPAM uses by default, these can be imported as custom properties. Click Add Custom Property to import a column, or Add All to import all columns.

6. Click Next.

7. The spreadsheet contents are validated. If errors are found, you are given the option to go back and fix these errors, import only the valid entries, or completely cancel the import.

8. Click Next.

9. On the Confirm choices page, click Import.

   The Import Summary page is displayed. Go to Complete the Import to continue.

Import only the Structure

1. The Subnet column matching page is displayed, showing the IPAM Subnet fields and what the wizard has determined to be the corresponding columns in the spreadsheet. If these are not correct or you do not want to import anything for a field, use the drop-down menu to select an alternative field.

   Select [Do not import] for fields that do not have a corresponding column in the spreadsheet.

   The only mandatory field is the Type.

2. Select option for where you want the imported subnets to go, and click Next:

   - IPAM will automatically create subnet hierarchy in selected location based on import file (hierarchy preserved)
   - IPAM will import subnets into the "Imported Subnet" folder (flat file structure)

3. If your spreadsheet contains additional columns to those IPAM uses by default, these can be imported as custom properties. Click Add Custom Property to import a column, or Add All to import all custom text fields.

4. Click Next.
5. The spreadsheet contents are validated. If errors are found, you are given the option to go back and fix the errors, import only the valid entries or cancel.
6. On the Confirm choices page, click Import.

   The Import Summary page is displayed. Go to Complete the Import to continue.

Import Structure and IP Address

1. The Subnet column matching page is displayed, showing the IPAM Subnet fields and what the wizard has determined to be the corresponding columns in the spreadsheet. If these are not correct or you do not want to import anything for a field, use the drop-down menu to select an alternative field.

   Select [Do not import] for fields that do not have a corresponding column in the spreadsheet.

   The only mandatory field is the Type.
2. Select the option for where you want the imported subnets to go, and click Next:
   - IPAM will automatically create subnet hierarchy in selected location based on import file (hierarchy preserved)
   - IPAM will import subnets into the "Imported Subnet" folder (flat file structure).
3. If your spreadsheet contains additional columns to those IPAM uses by default, these can be imported as custom properties. Click Add Custom Property to import a column, or Add All to import all custom text fields.
4. The spreadsheet contents are validated. If errors are found, you are given the option to go back and fix the errors, import only the valid entries or cancel.
5. Click Next.
6. The IP Address column matching page is displayed, showing the IPAM IP Address fields and what the wizard has determined to be the corresponding columns in the spreadsheet. If these are not correct or you do not want to import anything for a field, use the drop-down menu to select an alternative field.

   Select [Do not import] for fields that do not have a corresponding column in the spreadsheet.

   The only mandatory field is the IP Address.
7. Click Next.
8. On the Confirm choices page, click Import.

   The Import Summary is displayed.

Complete the import

The number of IP addresses that have been imported but have not been assigned to a parent subnet is displayed.

1. Click Next.

   If any IP addresses have been imported but have not been assigned to a subnet, the Assign Subnets to Ophaned IPs page is displayed.

   > ⓘ A warning banner will be displayed at the top of the Manage Subnets & IP Addresses page until all orphan IP addresses are assigned to subnets.

2. Select the IP Addresses you want to assign to specific subnet.

   - Select an IP Address and click Assign Subnet to create a subnet and assign subnets to this.
     - If you select an IPv4 address, all unassigned IPv4 addresses will be assigned to this subnet.
     - If you select an IPv6 address, all unassigned IPv6 addresses will be assigned to this subnet.

     You can hit Save to accept the default name and values and edit later, or set up any Subnet information here.

   - Click Assign IPs to Existing Subnets to add addresses to subnets that have already been created.

   The Manage Subnets & IP Addresses page is displayed showing the results of this import.

Add IPv6 addresses to IPAM

Adding IPv6 addresses to your network consists of the following three steps: create an IPv6 global prefix, create an IPv6 subnet, and then assign IPv6 addresses to this subnet.

> ⓘ Monitoring of IPv6 addresses is not available on Infoblox servers.

IPv6 addresses

An IPv6 address is represented by eight groups of four hexadecimal digits, each group representing 16 bits. Groups are separated by colons (:). For example:

```
10fa:6604:8136:05a2:73b0:0000:0000:0001
```

Representation can be simplified as follows:

Leading zeroes in a group may be omitted:

```
10fa:6604:8136:5a2:73b0:0:0:1
```

One or more consecutive groups containing zeros may be replaced by a single empty group, using two colons (::):

```
10fa:6604:8136:5a2:73b0::1
```

Create an IPv6 global prefix

An IPv6 address global prefix is a combination of an IPv6 prefix (address) and a prefix length. The prefix takes the form ipv6-prefix/prefix-length and represents a block of address space (or a network). The ipv6-prefix variable follows general IPv6 addressing rules.

The /prefix-length variable is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.

For example, `10fa:6604:8136:5a2:73b0::/64` is a possible IPv6 prefix.

1. Click My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Select a directory folder from the left menu tree, and then click Add > IPv6 Global Prefix.
3. Provide a name and description.
4. Enter the global prefix address.
5. Click Save.

> ⓘ After an IPv6 global prefix has been created and addresses have been assigned, you cannot edit the prefix. To change an IPv6 global prefix, you **must** delete the prefix and create a new one. If you have only created a prefix, you can click Edit to edit the prefix before you add addresses.

Create an IPv6 subnet

1. Click My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Select the IPv6 site under which you want to add the subnet.
3. Click Add IPv6 Subnet.
4. Enter a name, description, and IPv6 subnet address.
5. Click Save.

Assign IPv6 addresses

1. Click My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Expand the IPv6 site and select the a subnet to which you want to assign addresses.
3. Click Add IP Address.
4. Enter the IPv6 address, select a status, and add any further information.
5. Click Save.

Assign a subnet to an orphan IP address in IPAM

After you import IP addresses from a spreadsheet, it is possible that one or more IP addresses may have been imported without being assigned to a managed subnet. In order to properly manage your network, SolarWinds IPAM requires that all IP addresses are assigned to a managed subnet, even if the managed subnet contains only a single IP address.

If SolarWinds IPAM is unable to locate a configured subnet for each imported IP address, a warning banner is displayed.

The following procedure assigns parent subnets to orphaned IP addresses to enable their management by SolarWinds IPAM.

⚠ If you try to manage more IP addresses than your current license limit, IPAM adds as many IP addresses as it can. The remaining addresses are added as orphaned IP addresses.

1. Click Assign parent subnets to orphaned IPs in the warning banner.
2. Select a single orphaned IP address.
3. Click Assign Subnet.
4. If you do not want to use the default subnet name, enter a subnet name for the parent subnet. The default subnet name is made by connecting the subnet address and the CIDR prefix length.
5. If you do not want to use the default subnet address and CIDR prefix length provided by SolarWinds IPAM, enter a new subnet address and CIDR prefix length for the parent subnet.

   ⓘ SolarWinds IPAM suggests both a subnet address and a CIDR prefix length based on the orphaned IP address.

6. The Description, VLAN ID, and Location for the new parent subnet fields are optional.
7. Enter the Scan Interval.

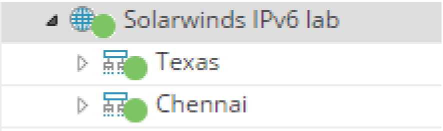
8. If you do not want SolarWinds IPAM to automatically scan your parent subnet for changes, select Disable Automatic Scanning.
9. Click Save.

Learn more about organizing IPv6 address spaces in IPAM

IPAM provides the ability to add IPv6 Sites and Subnets for planning purposes. IPv6 addresses can then be grouped to assist with network organization. To leverage the amount of addresses available, as well as the organizational features inherent with the implementation, you should create a logical address plan.

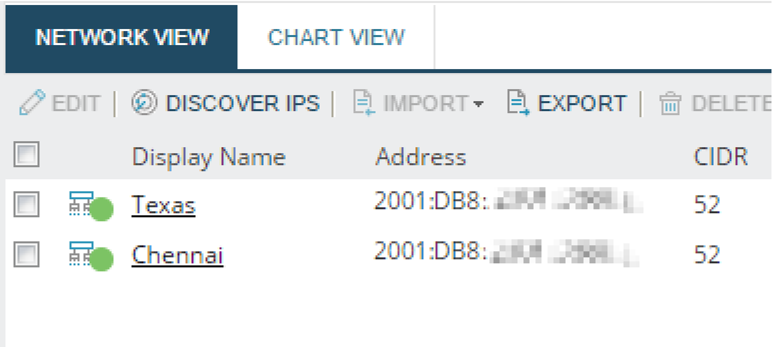
For example, you could designate two nibbles (a nibble is 4 bits or 1 hex character) for your country code. This will give you 2^8, or 256, possibilities for unique countries. Next, designate another nibble for state or location. Finally, designate bits for site, building, and floor.

Create an IPv6 Global site called SolarWinds v6 Lab.



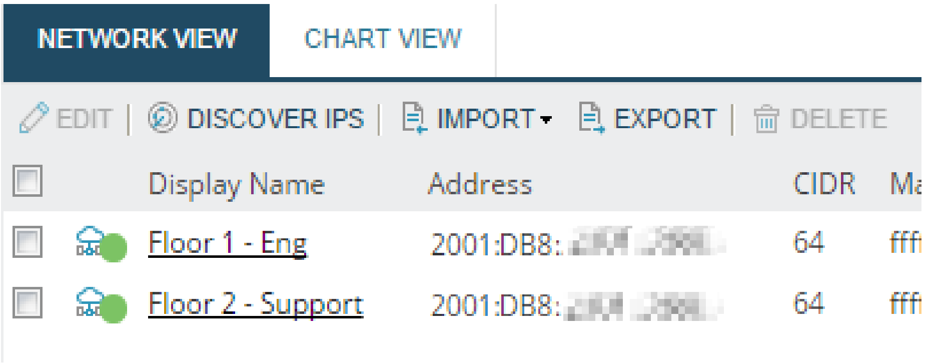
- Solarwinds IPv6 lab
  - Texas
  - Chennai

Then add Sites,



☐	Display Name	Address	CIDR
☐	Texas	2001:DB8:[redacted]	52
☐	Chennai	2001:DB8:[redacted]	52

Then add a building and floors.



☐	Display Name	Address	CIDR	Ma
☐	Floor 1 - Eng	2001:DB8:[redacted]	64	fff
☐	Floor 2 - Support	2001:DB8:[redacted]	64	fff

Manage Subnets and IP Addresses page

The Manage Subnets & IP Addresses page is the primary management interface for IPAM. The page is divided into two panes:

- The left pane provides a network tree representing the organization of your network into supernets, subnets, and groups.
- the right pane provides one of the following three views, depending on the type of network organization selected in the organization pane:
  - IP Address view
  - Network view
  - Chart view

See Manage subnets in IPAM for information about organizing your network with subnets.

See Manage supernets in IPAM for information about organizing your network with supernets.

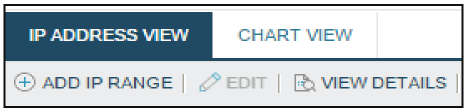
See IPAM groups for information about organizing your network with groups.

The following sections describe the information is available on each Manage Subnets & IP Addresses view.

The columns in the IP Address View and Network views can be hidden or displayed by moving the cursor over any column heading, clicking on the down arrow that then appears, selecting Add/Remove Columns, and selecting or deselecting the appropriate item. You can also drag and drop the columns into the order required. These changes will be retained for your login.

IP Address View

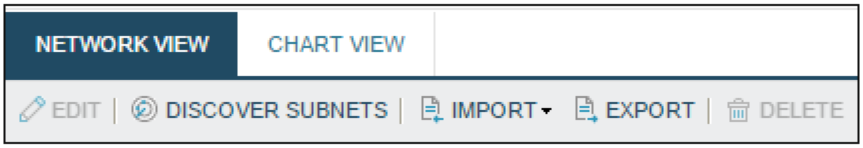
The IP Address View displays whenever a subnet is selected, either in the Network View on the right, or in the network organization pane on the left of the Manage Subnets & IP Addresses page. This view provides a list of all IP addresses that are within the selected subnet. This view can be filtered by selecting the DHCP Managed menu.



See IPAM status icons for more information about IP address iconsIPAM status icons Each IP address is listed with a selection of IP address properties. With the exception of Last Update, which is reported by IPAM as the result of a network scan, values for displayed IP address properties are set using the Edit IP Address window. See Add IP addresses to IPAM for more information about editing IP address properties.

Network View

The Network View displays whenever a group or supernet is selected in the network organization pane on the left of the Manage Subnets & IP Addresses page. If a group is selected, the view provides a list of all other groups, supernets, and subnets that are defined within the selected group. If a supernet is selected, the view provides a list of all subnets that are defined within the selected supernet. The Network tab also provides the ability to edit a single IP address and delete and import subnets by bulk.



The status of displayed network components is designated using colored icons.

See IPAM status icons for more information about network component icons.

With the exception of Last Discovery, which is reported by IPAM as the result of a network scan, values for displayed network component properties are set using the appropriate Edit Network Component Properties window. See IPAM groups for more information about editing group properties.

See Edit subnets for more information about editing subnet properties.

See Edit supernets for more information about editing supernet properties.

By default, only the first 150 items are displayed in each tree branch on the Manage Subnets & IP Addresses page. To change this, go to System Settings and change the Tree max items value as appropriate.

Chart View

The Chart View provides a concise, visual report of your IP address allocation for any network component selected in the network organization pane. It is on the right pane of the Manage Subnets & IP Addresses page. A pie chart displays the designated status of your monitored IP addresses. An availability report displays both the percentage of all possible IP addresses in the selected group, subnet, or supernet that are present for monitoring and the percentage of present IP addresses that are available for assignment.

See IPAM status icons for more information about IP address states in IPAM.

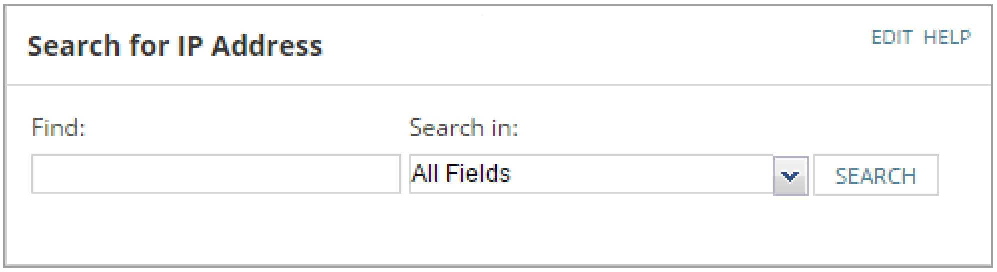
Manage IP addresses

This section includes the following topics:

Search for IP addresses in IPAM

Use the Search for IP Address widget to search multiple fields within your SolarWinds database for addresses managed with IPAM.

1. Click My Dashboards > IP Addresses > IPAM Summary.
2. On the Search for IP Address widget, select the field or fields to search in. You can select a single field, multiple fields or All Fields. The defaults are Alias, Hostname, IP Address, Dual Stack IPv6 Address and System Name.



Search for IP Address

Find:

Search in: All Fields

From IPAM 4.8, you can also search IPAM using the Search IPAM field in the upper right of the Manage Subnets & IP Addresses screen.

3. Enter a string or IP address to search for, and click Search.

   ⓘ Wildcards (*,?) are permitted, as shown in the following examples:

   - Cisco*
   - 10.15.*.*
   - W?ndows
   - Server-*
   - *.SolarWinds.com

   The IP Address Search page is displayed, listing the IP addresses that match your criteria.

4. Click a subnet or address to open the Manage Subnet & IP Addresses page with that subnet or IP address selected. From the IP Address view, you can click View Details to see the details page, or edit properties and set the status of the selected subnet or IP address.

IP Address Search

The IP Address Search pages provides the results of your IP search. The information for each IP address displayed will depend on its status.

You can choose to display only current IP address results or include historic results from any period over the last year.

- Click an IP or subnet address to display the Manage Subnets & IP Addresses page, showing the subnet with the IP address selected.
- Select a result and click Manage IP Address to display the Manage Subnets & IP Addresses page, showing the subnet with the IP address selected.
- Select a result and click View Details to display the IPAM IP Address Details page for this IP address.
- Select a result, click View Assignment History, and select:
  - IP Address Assignment History to display the IP Address History widget for this IP address.
  - MAC Assignment History to display the MAC Assignment History for the MAC address widget.
  - Hostname Assignment History to display the Hostname Assignment History widget for the hostname.

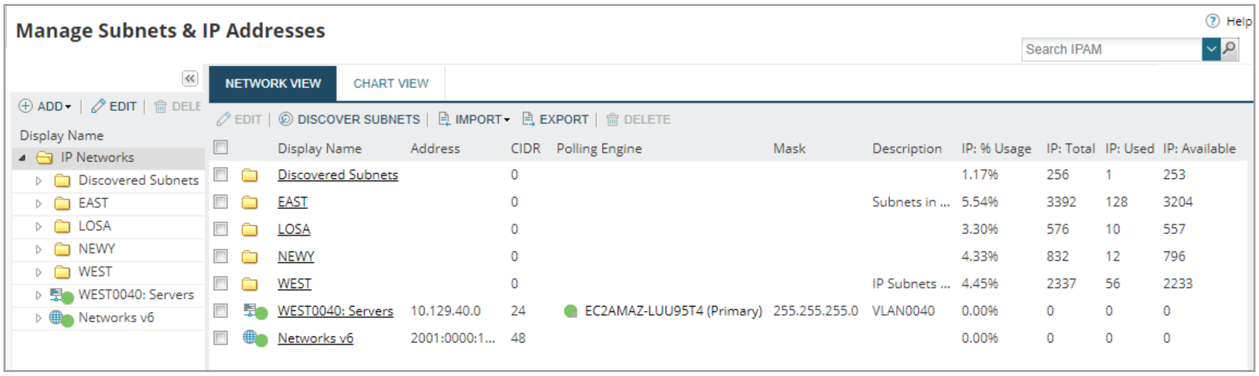
Edit IP Address page

IPAM maintains a wide array of information about the devices to which IP addresses are assigned, some of which is obtained when devices are polled, while other properties can be entered as required. You can Edit IP address properties directly from the IP Address view on the Manage Subnets & IP Addresses page, or from the IP Address Details widget on the IP Address Details page.

The following procedure shows how to edits the properties of an IP address within a defined subnet.

> If a defined subnet contains more than 4,096 IP addresses (lower than /20 or a 255.255.240.0 mask), IPAM only displays IP addresses in previously added ranges. For larger subnets, you must add IP address ranges for monitoring before IPAM can display addresses that may be managed.

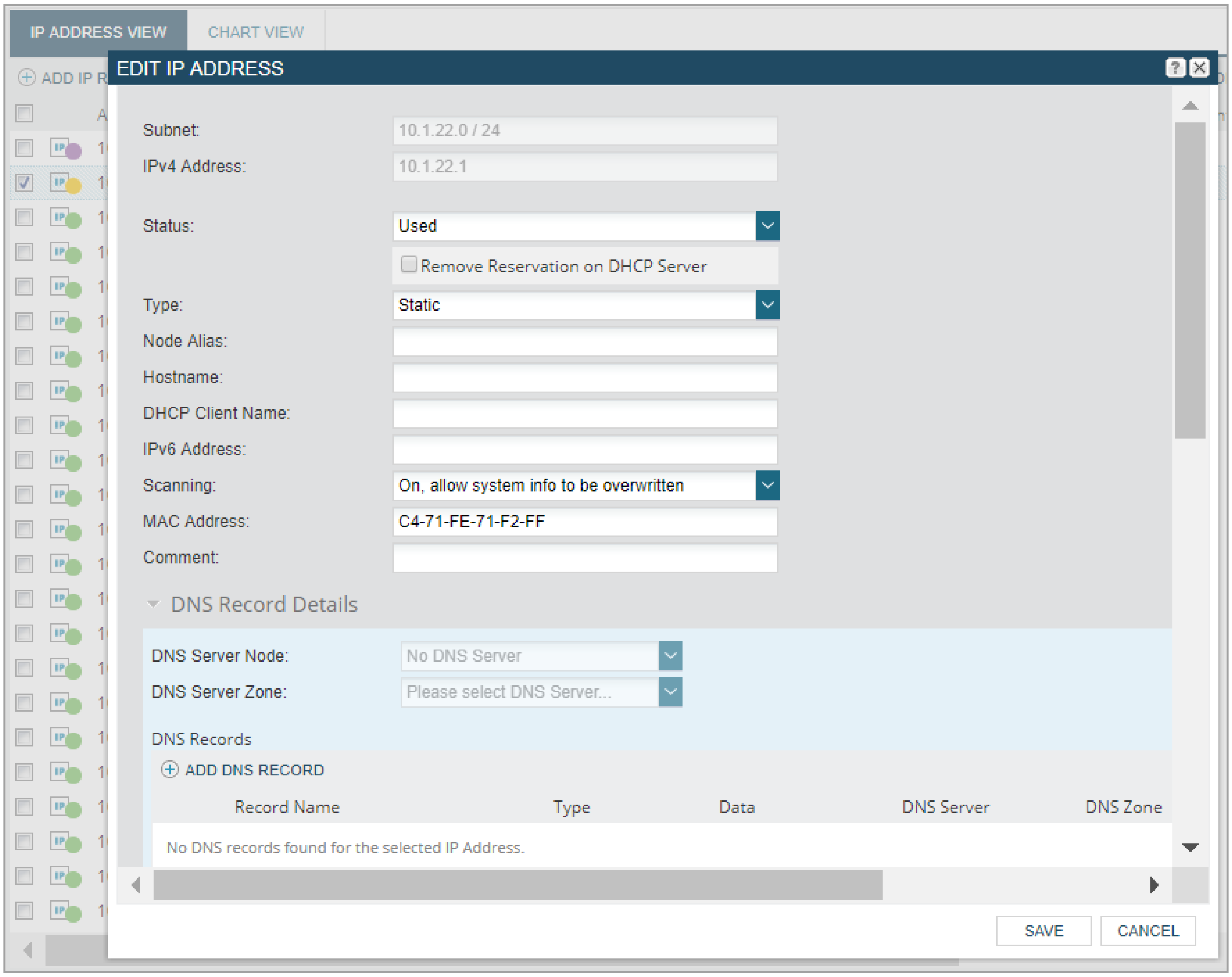
1. Navigate to My Dashboard > IP Addresses > Manage Subnets & IP Addresses.



□	Display Name	Address	CIDR	Polling Engine	Mask	Description	IP: % Usage	IP: Total	IP: Used	IP: Available
□	Discovered Subnets		0				1.17%	256	1	253
□	EAST		0			Subnets in ...	5.54%	3392	128	3204
□	LOSA		0				3.30%	576	10	557
□	NEWY		0				4.33%	832	12	796
□	WEST		0			IP Subnets ...	4.45%	2337	56	2233
□	WEST0040: Servers	10.129.40.0	24	● EC2AMAZ-LUU95T4 (Primary)	255.255.255.0	VLAN0040	0.00%	0	0	0
□	Networks v6	2001:0000:1...	48				0.00%	0	0	0

2. Expand the groups if necessary and click the subnet containing the IP address to edit.
3. Select the IP address to be edited in the right IP Address view pane, and click Edit.

4. The Edit IP Address page is displayed.



EDIT IP ADDRESS

Subnet:	10.1.22.0 / 24
IPv4 Address:	10.1.22.1
Status:	Used
	□ Remove Reservation on DHCP Server
Type:	Static
Node Alias:	
Hostname:	
DHCP Client Name:	
IPv6 Address:	
Scanning:	On, allow system info to be overwritten
MAC Address:	C4-71-FE-71-F2-FF
Comment:	

DNS Record Details

DNS Server Node:	No DNS Server
DNS Server Zone:	Please select DNS Server...

DNS Records

⊕ ADD DNS RECORD

Record Name	Type	Data	DNS Server	DNS Zone
No DNS records found for the selected IP Address.				

SAVE CANCEL

5. Edit the IP Address information as required.

   - The status field can also be set from the Network View using the Set Status drop-down.
   - Type - Static or Dynamic:
     - Static addresses will allow values to be overwritten.
     - Dynamic values will be overwritten (updated by the scanning engine)
   - IPv6 Address, as used for dual stack devices.

   > ⓘ A dual-stack device is a device with network interfaces that can originate and understand both IPv4 and IPv6 packets.

   - You can choose a DNS Server Zone to be associated with a subnet. This selected DNS zone acts like a filter, therefore DNS records not from the selected zone are shown as gray.
   - DNS details will be overwritten if forward lookup does not resolve.

- If you have defined custom properties for IP addresses, or want to add them, they can be added and edited from here.
- The DHCP Details and SNMP Details sections will be populated if the device associated with this IP address has been successfully polled. These fields are read-only.

6. Click Save when complete.

Edit or remove multiple IP address properties in IPAM

You can edit the properties of multiple IP addresses, enabling you to enter the same information for a range of addresses at once.

Edit multiple IP ranges

1. Click My Dashboard > IP Address Manager > Manage Subnets & IP Addresses.
2. Select the subnet you want to edit.
3. Click Select IP Range.
4. Enter the starting and ending IP addresses for the range.

   ⓘ You can only edit IP addresses of the same status.

5. Click Select + Edit to edit the properties.

   You can also select multiple IP addresses using the checkboxes and click Edit. This is useful if you want to select a non-contiguous range.

6. Edit or enter the properties you want the selected IP Addresses to have.

   The properties that can be edited depend on the status type of the selected IP Addresses.

7. Click Save.

ⓘ System Information is overwritten if scanning is enabled. Select Off to turn off automatic scanning from the Scanning menu.

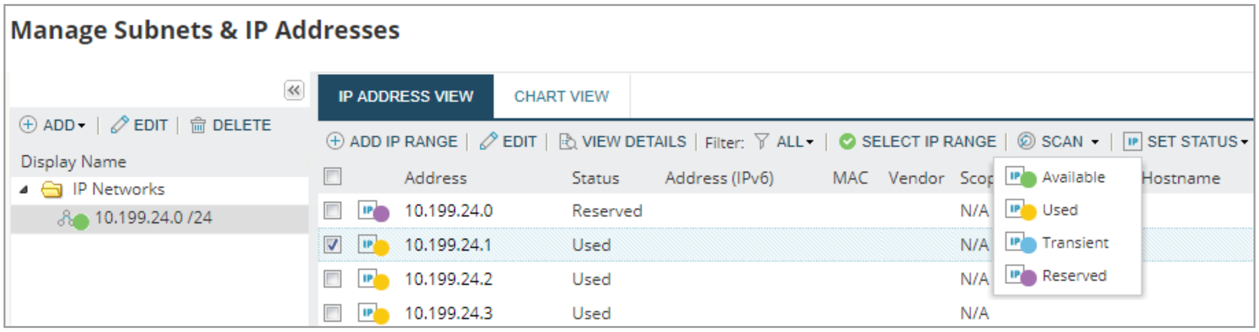
Remove multiple IP ranges

1. Click IP Address Manager > Manage Subnets & IP Addresses.
2. Select the subnet you want to edit.
3. Click Select IP Range.
4. Enter the starting and ending IP addresses for the range.

5. Click Select + Remove.
6. Click Yes to confirm.

Set an IP address status to Available, Used, Transient, or Reserved in IPAM

The status of any monitored IP address within a defined subnet may be set from the IP Address view on the Manage Subnets & IP Addresses page.



☐	Address	Status	Address (IPv6)	MAC	Vendor	Scop	Hostname
☐	10.199.24.0	Reserved				N/A	
☑	10.199.24.1	Used				N/A	
☐	10.199.24.2	Used				N/A	
☐	10.199.24.3	Used				N/A	

ⓘ If a subnet contains more than 4,096 IP addresses (lower than /20 or 255.255.240.0 mask), IPAM only displays IP addresses in previously added ranges. For larger subnets, you must add IP address ranges for monitoring before IPAM can display addresses that may be managed.

1. Click My Dashboards > Manage Subnets & IP Addresses.
2. Click the subnet.
3. Select the IP addresses to be modified.
4. Click Set Status and then select Available, Reserved, Transient or Used
   - Available: IP addresses currently unassigned to any network device.
   - Reserved: IP addresses typically located in blocks both at the beginning and at the end of any selected subnet. Reserved addresses may not be assigned to any network device.

     See Reserve an IP Address for instructions on how to reserve an IP address.
   - Transient: IP addresses typically associated with mobile devices that do not necessarily maintain continuous connection to the network.
   - Used: IP addresses currently assigned to a network device. As such, they may not be assigned to any other network device without first terminating their current assignment.

There is a fifth status icon: API Blocked. You cannot manually set an IP address status to API Blocked. This indicated an IP address is being modified by the IPAM API.

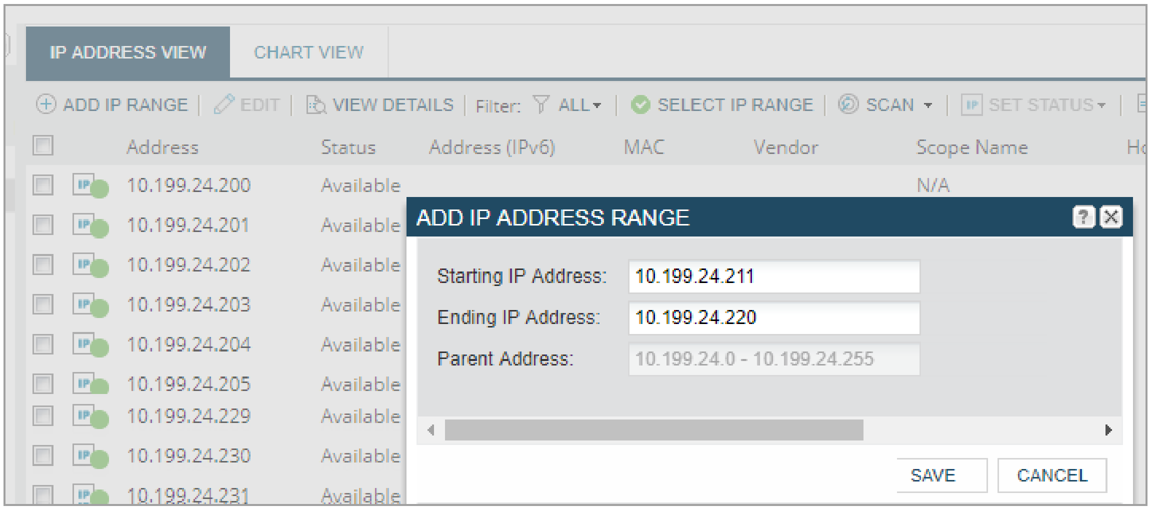
Create a range of IP addresses in a subnet

It can be useful to deal with IP addresses in terms of a defined IP address range within a subnet (for example,10.199.24.211 to 10.199.24.220 in a 10.199.24.0 / 24 subnet), especially when you have large subnets.

The following procedure adds a range of IP addresses within a defined subnet.

By default, IPAM displays all IP addresses in a subnet if the selected subnet contains 4,096 or fewer IP addresses (/20 or 255.255.240.0 and higher mask). For smaller subnets, it is not necessary to add IP address ranges for monitoring unless you have previously deleted the addresses in the range you want to add.

1. Click IP Address Manager > IP Addresses > Manage Subnets & IP Addresses.
2. In the network tree pane on the left, click the subnet to which you want to add your new IP address range.
3. Click Add IP Range.



Address	Status	Address (IPv6)	MAC	Vendor	Scope Name	Ho
10.199.24.200	Available				N/A	
10.199.24.201	Available					
10.199.24.202	Available					
10.199.24.203	Available					
10.199.24.204	Available					
10.199.24.205	Available					
10.199.24.229	Available					
10.199.24.230	Available					
10.199.24.231	Available					

Starting IP Address: 10.199.24.211
Ending IP Address: 10.199.24.220
Parent Address: 10.199.24.0 - 10.199.24.255

4. Enter the starting IP address and the ending IP address of your IP address range.

   IP address ranges cannot be defined outside the subnet indicated in the Parent Address field.

5. Click Save.

Organize an IP address space into IPAM subnets

Adding subnets to an existing or new supernet makes it easier to manage your network. Use the Subnet Allocation wizard to organize your managed IP address space into subnets.

> ⓘ Use the real-time subnet calculator to quickly determine the most efficient way to subdivide any supernet.

1. Click My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Click Add > Subnet Allocation Wizard.
3. Enter the address of the supernet to divide in the Supernet Address field.
4. Select a CIDR prefix length.
5. Select a subnet size.

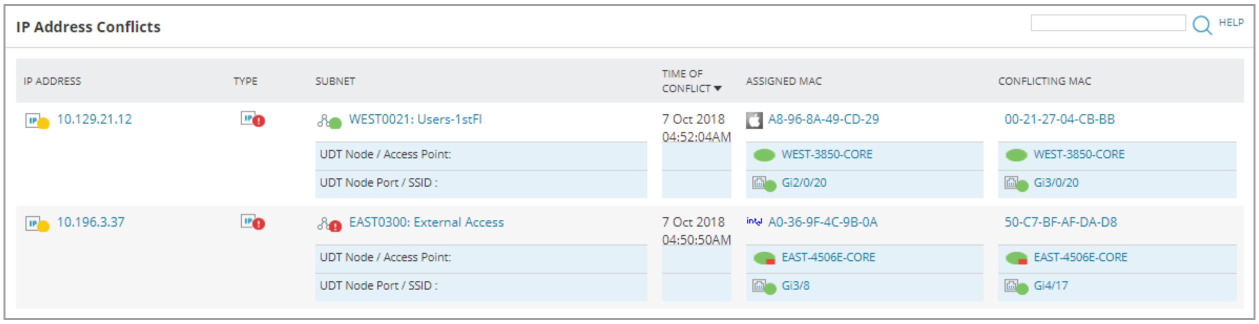
   > ⓘ Typically, in subnets defined to contain more than two IP addresses, the first and last addresses are reserved as the network address (to identify the subnet to the network) and the broadcast address (to communicate with all addresses within the subnet). As a result, the number of available IP addresses is always two fewer than the number actually contained within a given subnet.

6. To only see allocated subnets, clear Show subnets not already allocated.
7. Click Refresh to display a list of subnets that can be allocated based on your criteria.
8. Select the subnets you want to manage, and click Next.
9. (Optional) Enter a description, VLAN ID, and location for the subnets.
10. Select Disable Automatic Scanning to automatically scan the subnets for changes.
11. Click Done.

IP address conflicts

IPAM actively scans your network and if any duplicate static IP assignments or duplicate IP provisioning from a DHCP server are detected an event is triggered in the IP Address Conflicts widget on the IP Address Summary page. IPAM also detects if there is more than one MAC address using the same IP address within the same network. IPAM looks for differences in MAC addresses, from two distinct simultaneous scans for a single IP address, within a subnet.

The event information displays the IP address, conflict type, subnet, and MAC addresses that are in conflict, as shown below.



IP Address Conflicts HELP

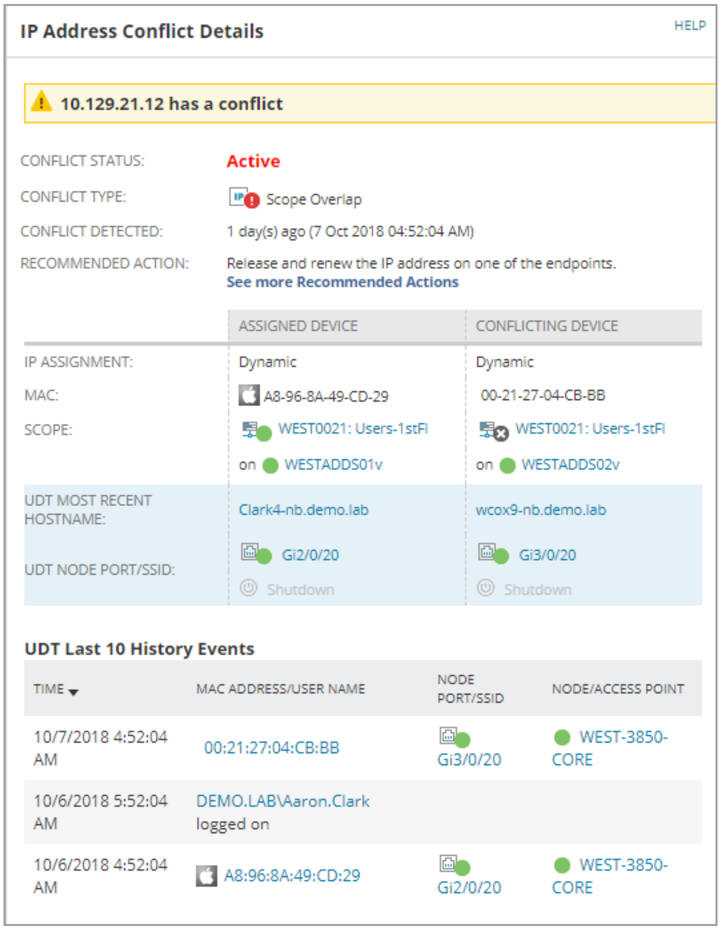
IP ADDRESS	TYPE	SUBNET	TIME OF CONFLICT ▾	ASSIGNED MAC	CONFLICTING MAC
10.129.21.12		WEST0021: Users-1stFl	7 Oct 2018 04:52:04AM	A8-96-8A-49-CD-29	00-21-27-04-CB-BB
		UDT Node / Access Point:		WEST-3850-CORE	WEST-3850-CORE
		UDT Node Port / SSID :		Gi2/0/20	Gi3/0/20
10.196.3.37		EAST0300: External Access	7 Oct 2018 04:50:50AM	A0-36-9F-4C-9B-0A	50-C7-BF-AF-DA-D8
		UDT Node / Access Point:		EAST-4506E-CORE	EAST-4506E-CORE
		UDT Node Port / SSID :		Gi3/8	Gi4/17

Here, two devices on the WEST0021 subnet (and two on the EAST0300 subnet) are in conflict.

Move the cursor over the Type icon to show the conflict type (for example, Scope overlap, Dynamic + Static)

ⓘ If UDT is installed additional information is displayed, showing node and node port details.

Click on an IP address to show the IPAM IP Address Details page. The IP Address Conflict Details widget shown below is displayed.



IP Address Conflict Details HELP

⚠ **10.129.21.12 has a conflict**

CONFLICT STATUS: **Active**

CONFLICT TYPE: Scope Overlap

CONFLICT DETECTED: 1 day(s) ago (7 Oct 2018 04:52:04 AM)

RECOMMENDED ACTION: Release and renew the IP address on one of the endpoints.
See more Recommended Actions

	ASSIGNED DEVICE	CONFLICTING DEVICE
IP ASSIGNMENT:	Dynamic	Dynamic
MAC:	A8-96-8A-49-CD-29	00-21-27-04-CB-BB
SCOPE:	WEST0021: Users-1stFl on ● WESTADDS01v	WEST0021: Users-1stFl on ● WESTADDS02v
UDT MOST RECENT HOSTNAME:	Clark4-nb.demo.lab	wcox9-nb.demo.lab
UDT NODE PORT/SSID:	Gi2/0/20 Shutdown	Gi3/0/20 Shutdown

UDT Last 10 History Events

TIME ▾	MAC ADDRESS/USER NAME	NODE PORT/SSID	NODE/ACCESS POINT
10/7/2018 4:52:04 AM	00:21:27:04:CB:BB	Gi3/0/20	● WEST-3850-CORE
10/6/2018 5:52:04 AM	DEMO.LAB\Aaron.Clark logged on		
10/6/2018 4:52:04 AM	A8:96:8A:49:CD:29	Gi2/0/20	● WEST-3850-CORE

Recommended action is displayed. Click See more Recommended Actions to display further actions.

See the table below for further information about the different kinds of IP Address conflict and how to remedy these.

> If UDT is installed, this widget will show the last ten events for this IP address enabling you to track down the cause and responsibility for the conflict.

IP address conflict scenarios

IPAM automatically detects IP conflicts by scanning servers and devices, and alerts you when conflicts are found. IPAM alerts for the following IP address conflict scenarios.

> During subnet scans, MAC addresses obtained from SNMP, SNMP neighbor, and IPAM reservations are called Static entries and those obtained from DHCP servers are called Dynamic entries.

The different kinds of IP address conflicts are:

Type		Description	Remedy
Static and Static	SNMP versus SNMP Neighbor	There is a conflict in the MAC addresses retrieved from the ARP table of the configured device and from the SNMP OIDs during the subnet scan for an IP address.	1. Try to remotely connect to one of the assigned or conflicting machines using RDP and change the IP address to one that's current free in IPAM within the same subnet. 2. If device(s) connected via WiFi, connect to AP and block conflicting MAC address and change IP locally on the device. 3. You may shut down a port on a switch for one of assigned or conflicting MAC and change IP locally on the device.
	IPAM reservation versus SNMP/SNMP neighbor	There are situations where you reserve an IP address under a subnet in IPAM that contains a MAC address for an internal reference. This type of conflict occurs when there is a difference in MAC addressees from either SNMP OIDs, or neighbor devices with reserved MAC addresses in IPAM.	

Type		Description	Remedy
Static and Dynamic	SNMP versus DHCP	There is a difference in the MAC addresses fetched from an SNMP OID and DHCP leases from a DHCP server, for an IP address during a subnet scan.	1. Try to remotely connect to the machine with static IP via RDP and change the IP address from “static” to “obtained via DHCP server”. 2. If device(s) connected via WiFi, connect to AP and block static IP address and change IP locally on the device. 3. You may shut down a port on a switch for one of statically assigned IP & MAC and change IP locally on the device. 4. In a case DHCP assigns wrong IP, try to update DHCP firmware.
	SNMP Neighbor versus DHCP	There is a difference in the MAC addresses retrieved from the ARP table of the configured device and from DHCP leases from the DHCP server.	
	IPAM reservation versus DHCP	There are situations where you reserve an IP address under a subnet in IPAM that contains a MAC address for an internal reference. This type of conflict occurs when there is a difference in MAC addressees from DHCP leases with reserved MAC addresses in IPAM.	

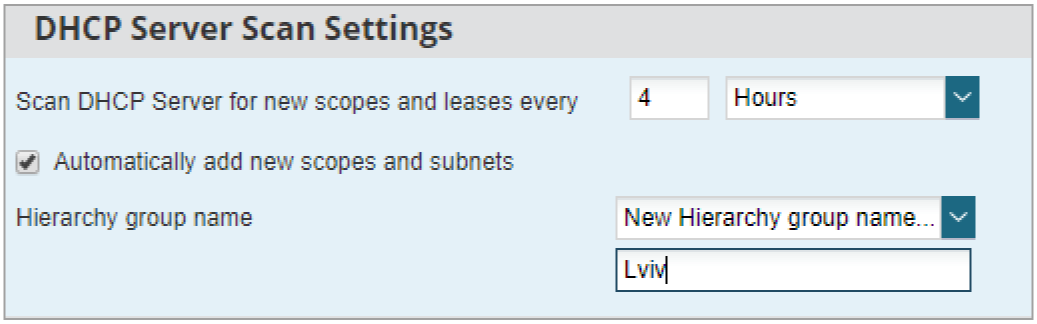
Type		Description	Remedy
Dynamic and Dynamic	DHCP versus DHCP	A range of IP addresses within a subnet may be managed by two DHCP servers. This conflict occurs when there is a difference in MAC addresses retrieved from the two DHCP servers' lease information.	1. Try to remotely connect via RDP to one of machines in conflict and change IP address to static to free IP in a subnet. Then re-size DHCP scopes so they are not overlapping and reset static IP to dynamic on the device. 2. Shut down a port on a switch for conflicting IP and e-size DHCP scopes so they are not overlapping. Then enable blocked port again.
	DHCP versus DHCP (scope overlap)	A range of IP addresses within a subnet may be managed by two DHCP servers. There are cases when a part of an IP address range under one DHCP server is managed by another DHCP server. In both instances, there is an overlap in scopes between two DHCP servers. This is considered a conflict.	

Remove monitored IP addresses from a subnet

1. Click My Dashboards > IP Address Manager > Manage Subnets & IP Addresses.
2. Click the subnet from which you want to delete a range of IP addresses.
3. Click Select IP Range.
4. Enter the start and end IP addresses.
5. Click Select + Remove.
6. Click Yes to confirm the deletion, and click Save.

Overlapping IP addresses and hierarchy groups in IPAM

An overlapping IP address occurs when an IP address is assigned to more than one device on a network. This can happen if you have identical subnets in different locations monitored by different DHCP servers on the same network. To avoid IP conflicts when subnets are automatically discovered, you can designate an hierarchy group to which all discovered subnets are assigned when you add a DHCP Server.



DHCP Server Scan Settings

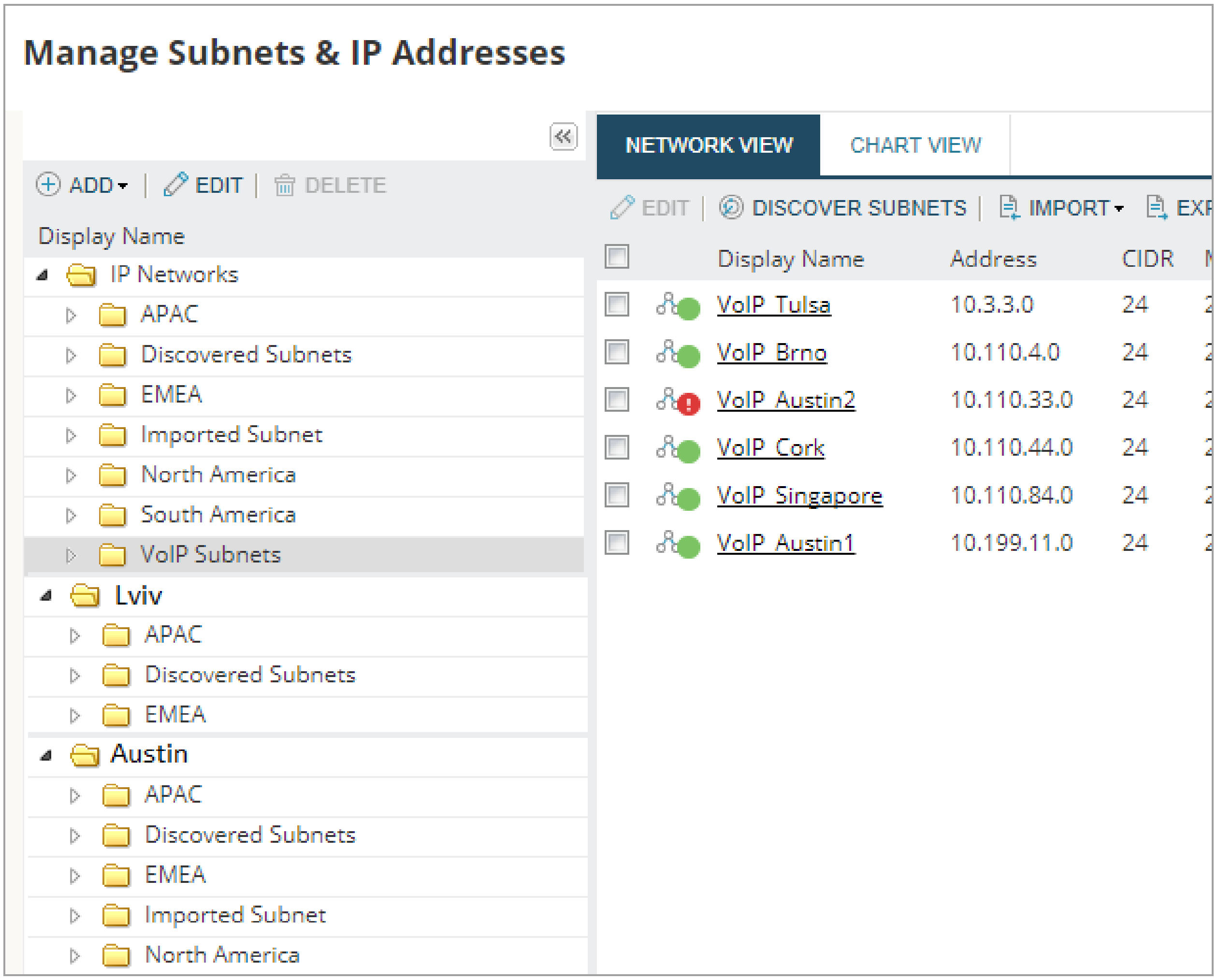
Scan DHCP Server for new scopes and leases every: 4 Hours

☑ Automatically add new scopes and subnets

Hierarchy group name: New Hierarchy group name... — Lviv

If a hierarchy group name is not selected, all discovered subnets for a DHCP Server go to the IP Networks hierarchy group.

IP conflicts are only detected if they occur in the bounds of the same hierarchy group.



Manage Subnets & IP Addresses

Display Name

- IP Networks
  - APAC
  - Discovered Subnets
  - EMEA
  - Imported Subnet
  - North America
  - South America
  - VoIP Subnets
- Lviv
  - APAC
  - Discovered Subnets
  - EMEA
- Austin
  - APAC
  - Discovered Subnets
  - EMEA
  - Imported Subnet
  - North America

□	Display Name	Address	CIDR
□	VoIP_Tulsa	10.3.3.0	24
□	VoIP_Brno	10.110.4.0	24
□	VoIP_Austin2	10.110.33.0	24
□	VoIP_Cork	10.110.44.0	24
□	VoIP_Singapore	10.110.84.0	24
□	VoIP_Austin1	10.199.11.0	24

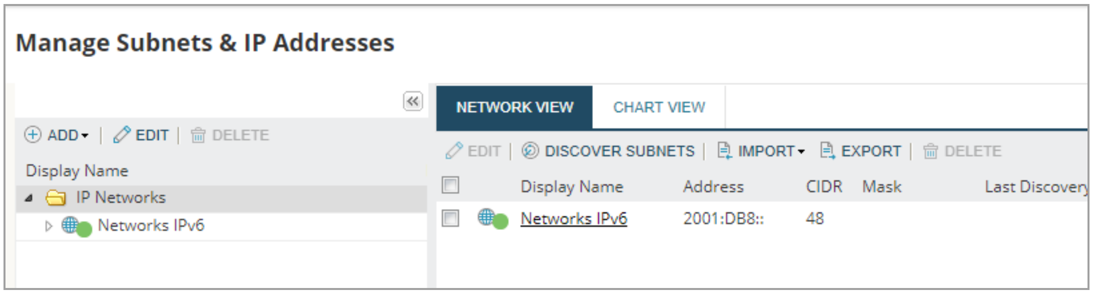
Subnets cannot be moved between hierarchy groups.

Adding IPv6 addresses to IPAM

IPAM lets you add IPv6 (Internet Protocol version 6) sites to subnets to be monitored. Use the Discover IPs functionality to automatically add existing IP addresses to subnets.

IPv6 addresses can be grouped to assist with network organization. To leverage the amount of addresses available, as well as the organizational features inherent with the implementation, create a logical address plan. For example, designate two nibbles (a nibble is 4 bits or 1 hex character) for your country code. This is 2^8, or 256, possibilities for unique countries. Next, designate another nibble for state or location. Finally, designate bits for site, building, and floor.

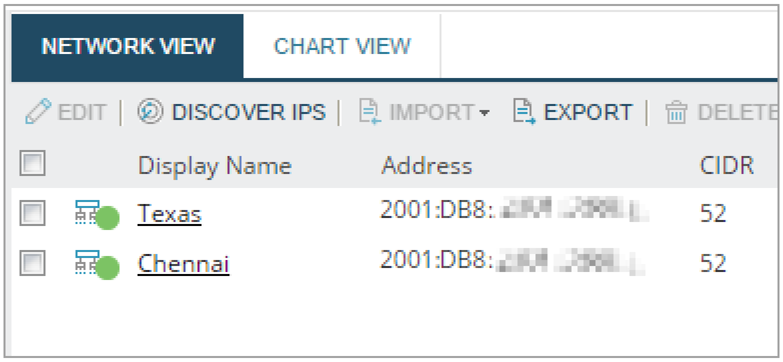
1. Go to My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Click Add and select IPv6 Global Prefix.
3. Create an IPv6 Global site. For this you require a name and a global prefix address.



Manage Subnets & IP Addresses

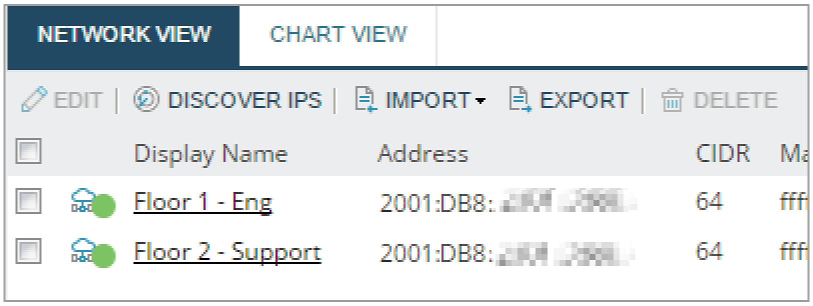
□		Display Name	Address	CIDR	Mask	Last Discovery
□		Networks IPv6	2001:DB8::	48		

4. Select this site, click Add, and select IPv6 Site.
5. Add your IPv6 sites.



□		Display Name	Address	CIDR
□		Texas	2001:DB8:[redacted]	52
□		Chennai	2001:DB8:[redacted]	52

6. Add a building and floors.



□		Display Name	Address	CIDR	Ma
□		Floor 1 - Eng	2001:DB8:[redacted]	64	fff
□		Floor 2 - Support	2001:DB8:[redacted]	64	fff

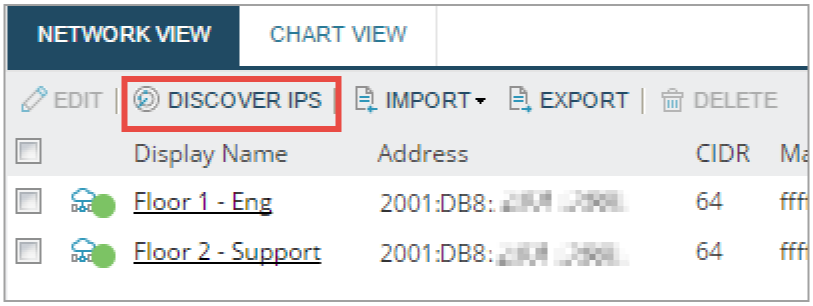
IPv6 scanning

IPAM IPv6 address discovery uses Neighborhood Discovery Protocol (NDP). Information is obtained from routers based on the following MIBs and OIDs:

- IPv6 MIB, OID 1.3.6.1.2.1.55.1.12.1.2 (ipv6NetToMediaTablePhysicalAddress)
- IP MIB, OID 1.3.6.1.2.1.4.35 (ipNetToPhysicalTable)
- ipv6NetToMediaValid - 1.3.6.1.2.1.55.1.12.1.6
- Cisco proprietary CISCO-IETF-IP-MIB , OID 1.3.6.1.4.1.9.10.86.1.1.3 (clnetNetToMediaTable)

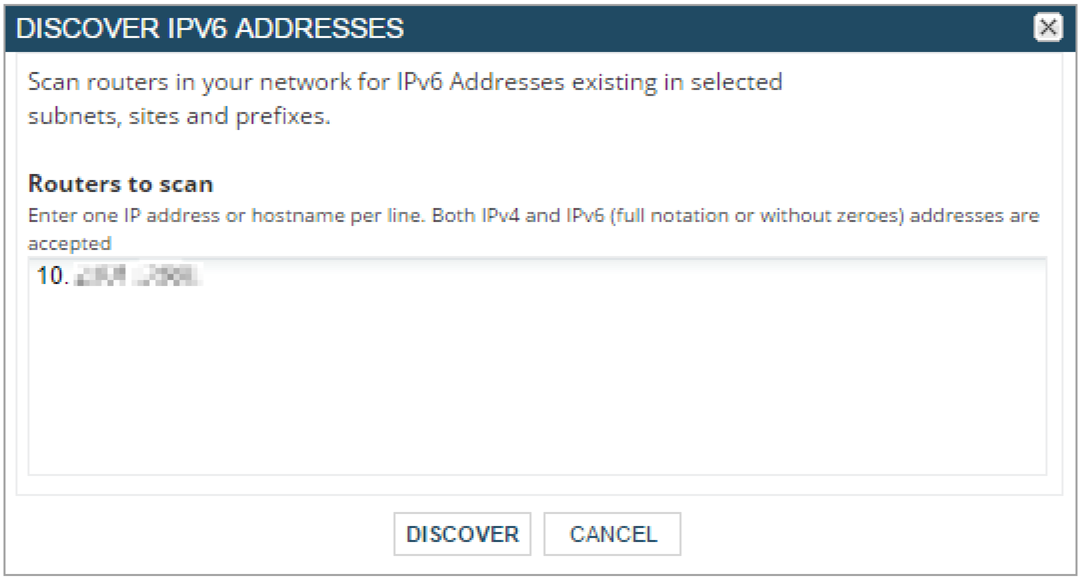
ⓘ For troubleshooting, verify with these device OIDs.

1. Click Discover IPs to access this functionality from the IPv6 subnet(s) or IPv6 Global prefix menus.



□		Display Name	Address	CIDR	Ma
□		Floor 1 - Eng	2001:DB8:[redacted]	64	fff
□		Floor 2 - Support	2001:DB8:[redacted]	64	fff

2. Select the routers to scan.



Scan routers in your network for IPv6 Addresses existing in selected subnets, sites and prefixes.

Routers to scan

Enter one IP address or hostname per line. Both IPv4 and IPv6 (full notation or without zeroes) addresses are accepted

10.[redacted]

The discovery populates all discovered IPs under their IPv6 subnet(s) in the selection. All found IPs that do not belong to a selected subnet are discarded. IPAM uses your SNMP credentials to access the selected routers.

IP address requests

The IP Request feature in IPAM allows anyone within your network to request IP addresses and gives the IPAM administrator a convenient method to review and assign IPs as requested. With the 2020.2.6 release IPAM provides additional options for administrators to work with the IP Request process. This new implementation covers the previous use cases and adds further security and workflow options.

All IPAM administrators should review these new options and adapt the one that best fits their needs.

> If you are upgrading from previous versions:
>
> - This change to the IP request process removes the previous method of providing a username/password combination for the IP Address Request form.
> - If you were using that method, your network will no longer have access to the IP Address Request form until you select one of the three options.

See:

- The new IP Request form access settings
  - ○ IP Request Access: Restricted
  - ○ IP Request Access: Users with access token
  - ○ IP Request Access: All users
- Request an IP Address using the IP Request link
- Request an IP address with IPAM access
- Process IP address requests
- The IPAM - All Created IP Requests report
- IP Request Settings

The new IP Request form access settings

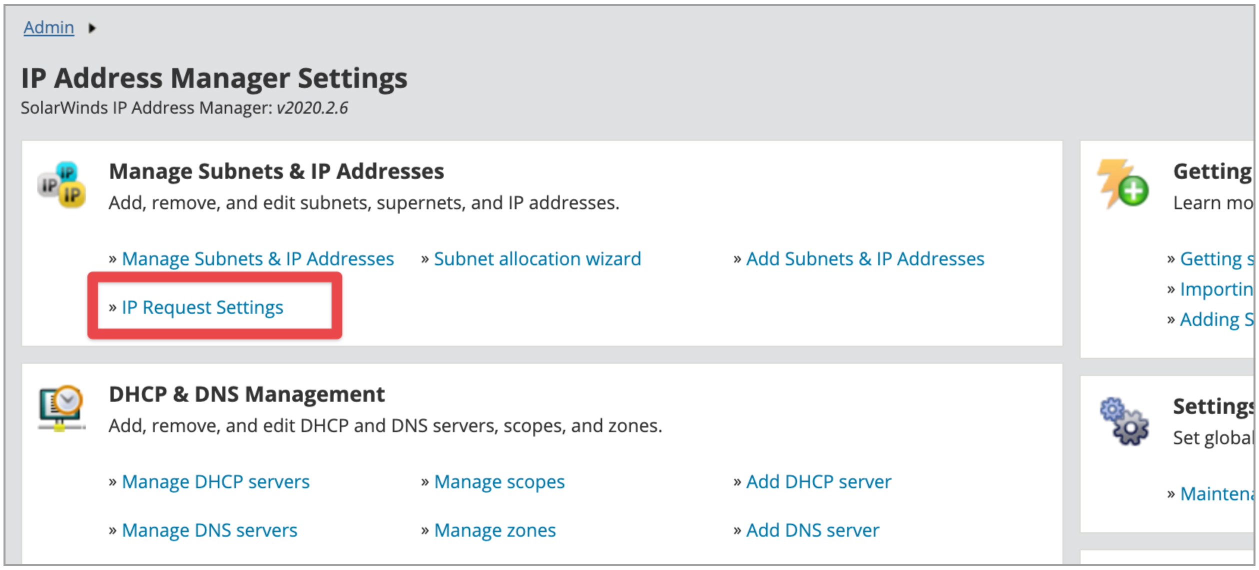
The new options can be found at the head of the IP Request page.

1. From the SolarWinds web console menu, select Settings > All Settings.

   The Main Settings & Administration page is displayed.

2. In the Product Specific Settings section, click IPAM Settings.

   The IP Address Manager Settings page is displayed.



Admin ▸

IP Address Manager Settings

SolarWinds IP Address Manager: *v2020.2.6*

Manage Subnets & IP Addresses

Add, remove, and edit subnets, supernets, and IP addresses.

» Manage Subnets & IP Addresses » Subnet allocation wizard » Add Subnets & IP Addresses

» IP Request Settings

DHCP & DNS Management

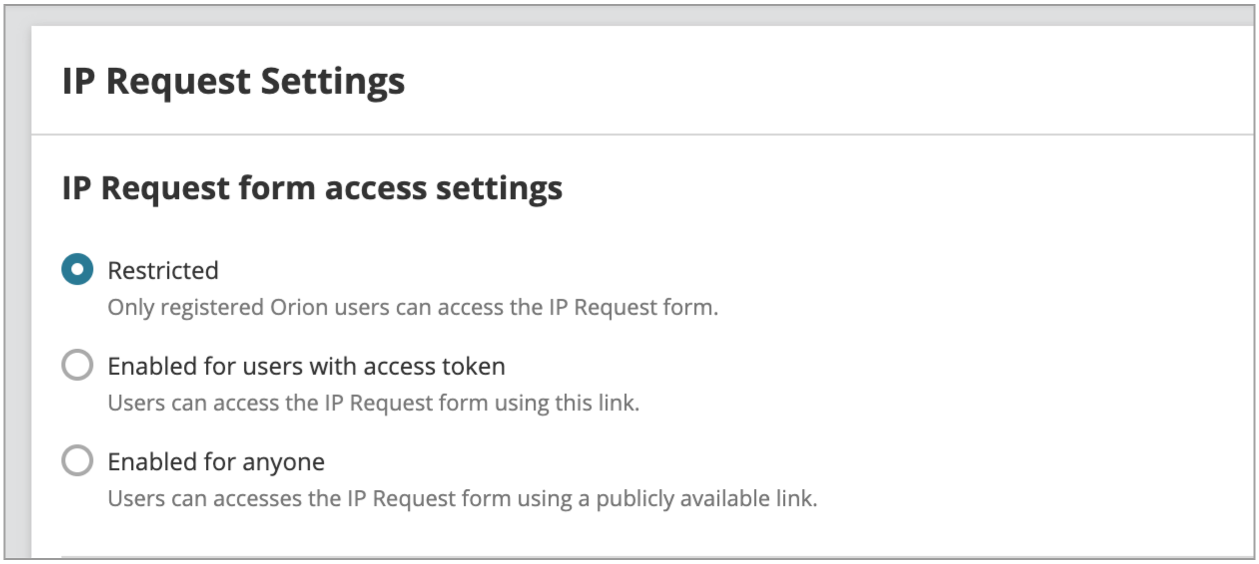
Add, remove, and edit DHCP and DNS servers, scopes, and zones.

» Manage DHCP servers » Manage scopes » Add DHCP server

» Manage DNS servers » Manage zones » Add DNS server

3. In the Manage Subnets & IP Addresses section, click IP Request Settings.

   The IP Request Settings page is displayed with the IP Request form access settings at the top.



IP Request Settings

IP Request form access settings

● Restricted
Only registered Orion users can access the IP Request form.

○ Enabled for users with access token
Users can access the IP Request form using this link.

○ Enabled for anyone
Users can accesses the IP Request form using a publicly available link.

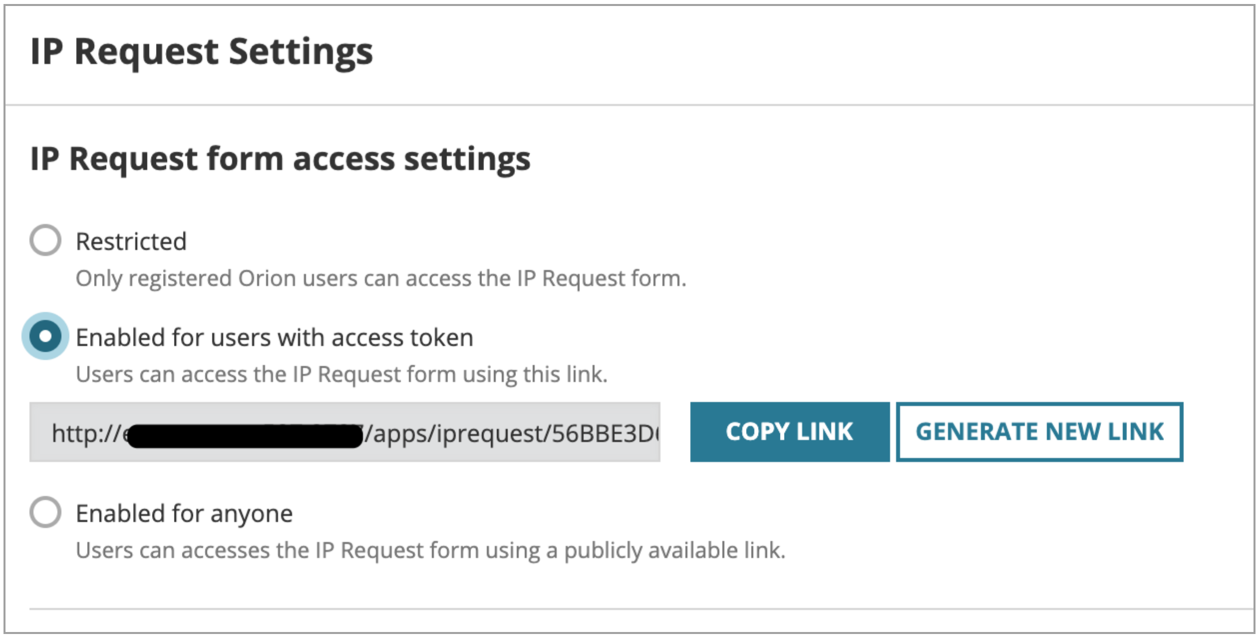
Summary of options

You have three options for how you want to work with the IP request process. Click on the option name for further information:

Option	Description
Restricted	If this option is selected, only users with IPAM accounts (and who are logged into this account) can access the IP Address Request form. This is done through My Dashboards > IP Addresses > Request IP Address.

Option	Description
Enabled for users with access token	If this option is selected, users in your network will need the URL and access token provided by you to access the IP Address Request form. Users with IPAM account can access the form through My Dashboards > IP Addresses > Request IP Address.
Enabled for anyone	If this option is selected, users in your network will need the URL provided by you to access the IP Address Request form. Use this option to reduce friction for your users when requesting IP addresses. Users with an IPAM account can access the form through My Dashboards > IP Addresses > Request IP Address.

IP Request Access: Users with access token



IP Request Settings

IP Request form access settings

○ Restricted
Only registered Orion users can access the IP Request form.

● Enabled for users with access token
Users can access the IP Request form using this link.

http://[redacted]/apps/iprequest/56BBE3D

○ Enabled for anyone
Users can accesses the IP Request form using a publicly available link.

With this option, the IP Request form is presented as a separate public application accessible to people in your network who have been given the page's URL and access token. An SolarWinds account is not required to access this feature.

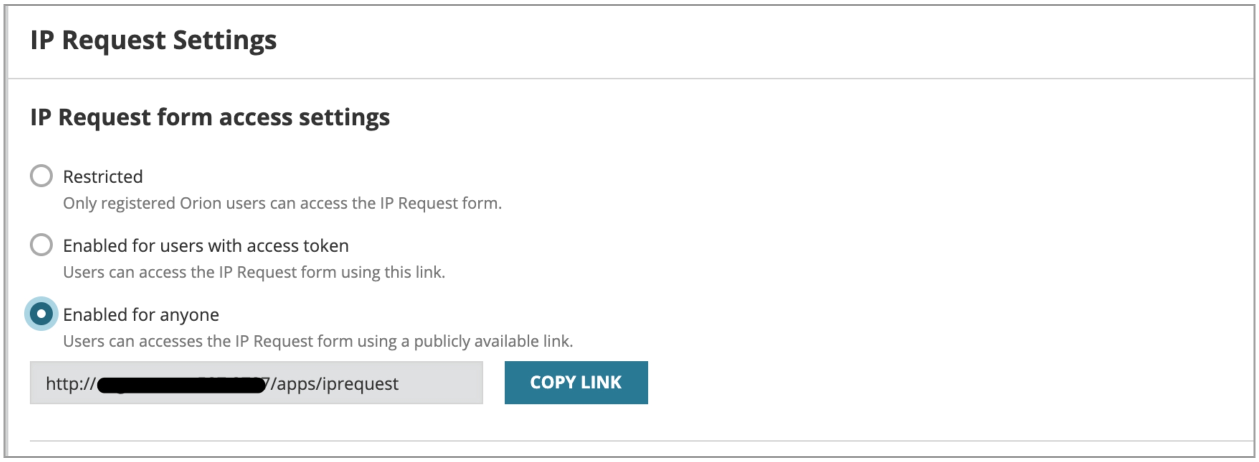
This feature provide extra security by enabling you to regenerate a new access token at any time. This is especially useful if you are periodically changing access credentials in your network, or in response to a particular security event.

SolarWinds web console users are still able to access the private request form via the SolarWinds web console menu.

ⓘ Users with permission to view subnet options in the IP request form should access it via the SolarWinds web console menu rather than using the link as subnets are not displayed when the IP Request form is accessed through the link.

IP Request Access: All users

Enabled for anyone



IP Request Settings

IP Request form access settings

○ Restricted
Only registered Orion users can access the IP Request form.

○ Enabled for users with access token
Users can access the IP Request form using this link.

● Enabled for anyone
Users can accesses the IP Request form using a publicly available link.

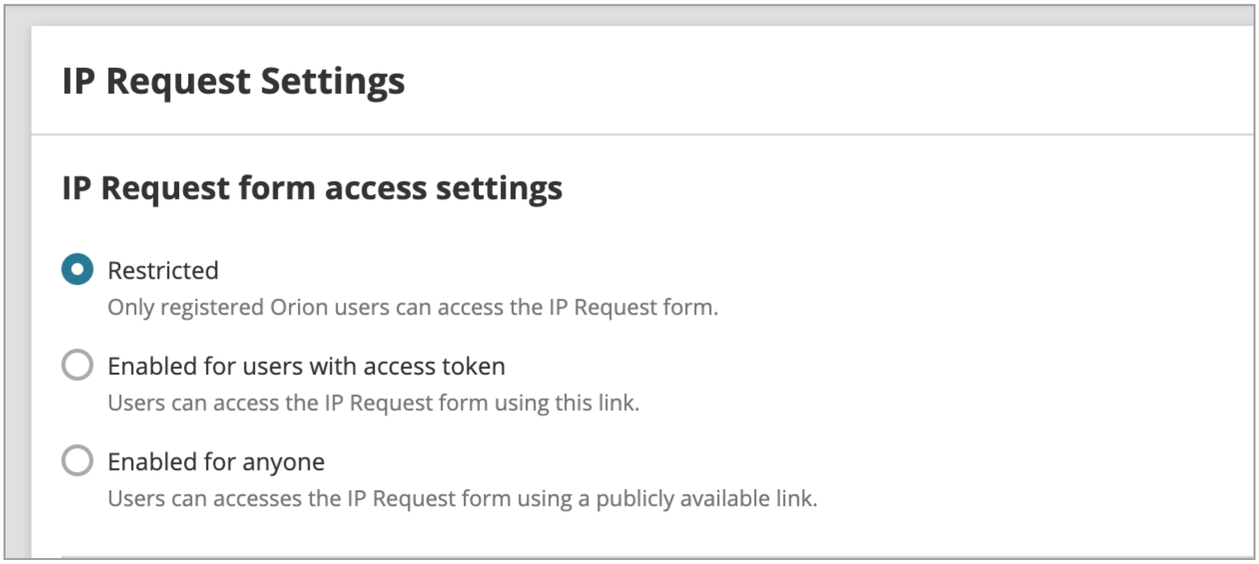
http://[redacted]/apps/iprequest

This option provides a separate public application similar to the previous option but the difference is the link structure ends with a static "/apps/iprequest". It is not possible to change this link or update it. Team members in your network can bookmark this link and know it will always work as long as the "enabled for anyone" option is selected.

SolarWinds web console users are still able to access the private request form via the SolarWinds web console menu.

ⓘ Users with permission to view subnet options in the IP request form should access it via the SolarWinds web console menu rather than using the link as subnets are not displayed when the IP Request form is accessed through the link.

IP Request Access: Restricted



IP Request Settings

IP Request form access settings

● Restricted
Only registered Orion users can access the IP Request form.

○ Enabled for users with access token
Users can access the IP Request form using this link.

○ Enabled for anyone
Users can accesses the IP Request form using a publicly available link.

When you upgrade or install IPAM, this will be the default option as it provides the most security of the three options.

To request IP addresses, a team member will need to have a login for the SolarWinds web console and will need to be logged in.

If a user is not logged in, they will be redirected to the IPAM login page.

Users with any IPAM role will have access to the IP request page, but some parts of the IP Request form may be restricted and not shown (for example, where subnets are displayed), depending upon their IPAM permissions.

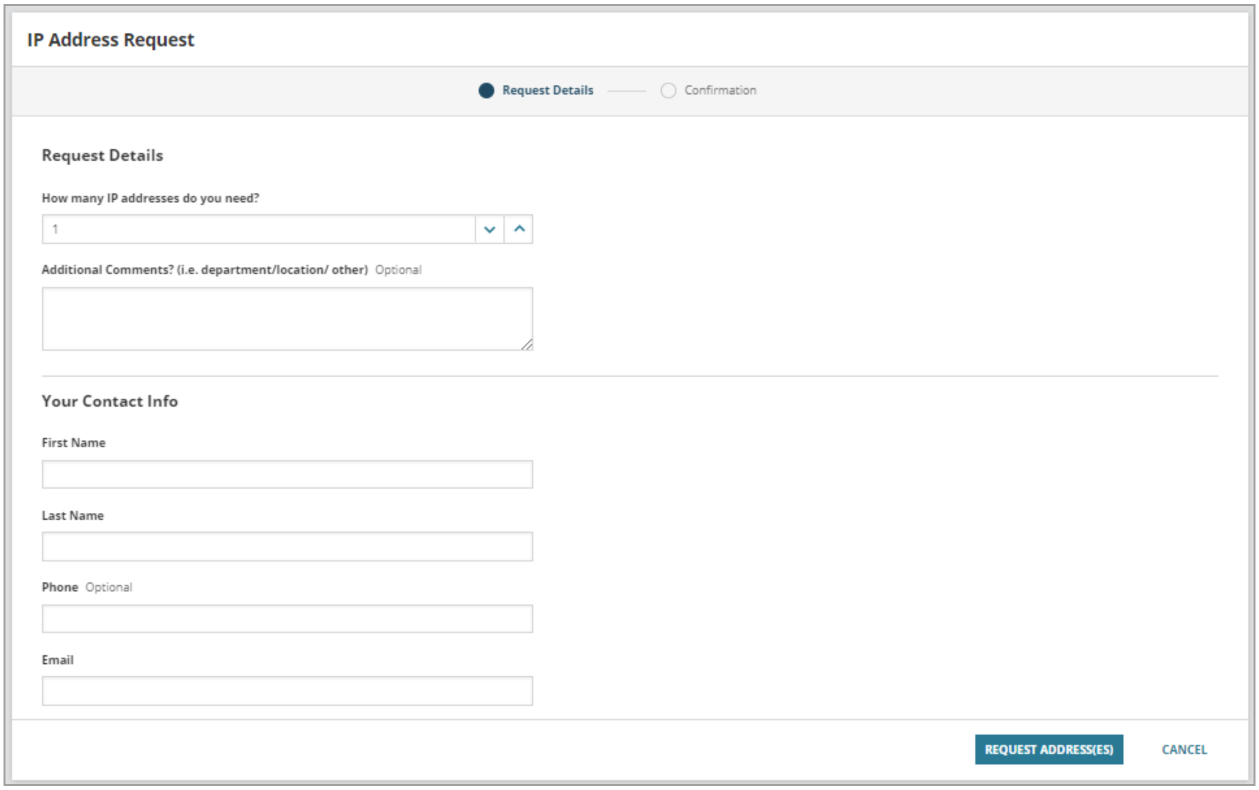
Request an IP Address using the IP Request link

When a user without an IPAM login requires one or more IP addresses, they should use the following procedure:

> ⓘ The user will need an IP Request link. This will either be static or will end with an access token depending on the security option in force.
>
> For example:
>
> - `https://amadeupcompanyinaustin.com/apps/iprequest` - if it is a static link
> - `https://amadeupcompanyinaustin.com/apps/iprequest/ABCD9999` - if an access token is required
>
> The user should contact their IPAM administrator if they do not have this link or it does not work.

1. Enter the IP Request link in the address bar of the browser.

   The IP Address Request page is displayed.



IP Address Request

Request Details

How many IP addresses do you need?: 1

Additional Comments? (i.e. department/location/ other) Optional

Your Contact Info

First Name

Last Name

Phone Optional

Email

2. Select the number of IP addresses required.
3. (Optional) Enter any comments regarding this request.
4. Enter contact information, and click Request Address(es).

   All fields except those marked as Optional must be completed.

   When the user clicks Request Address(es) a conformation message is displayed, telling them their request has been sent to the administrator and they will be contacted shortly.

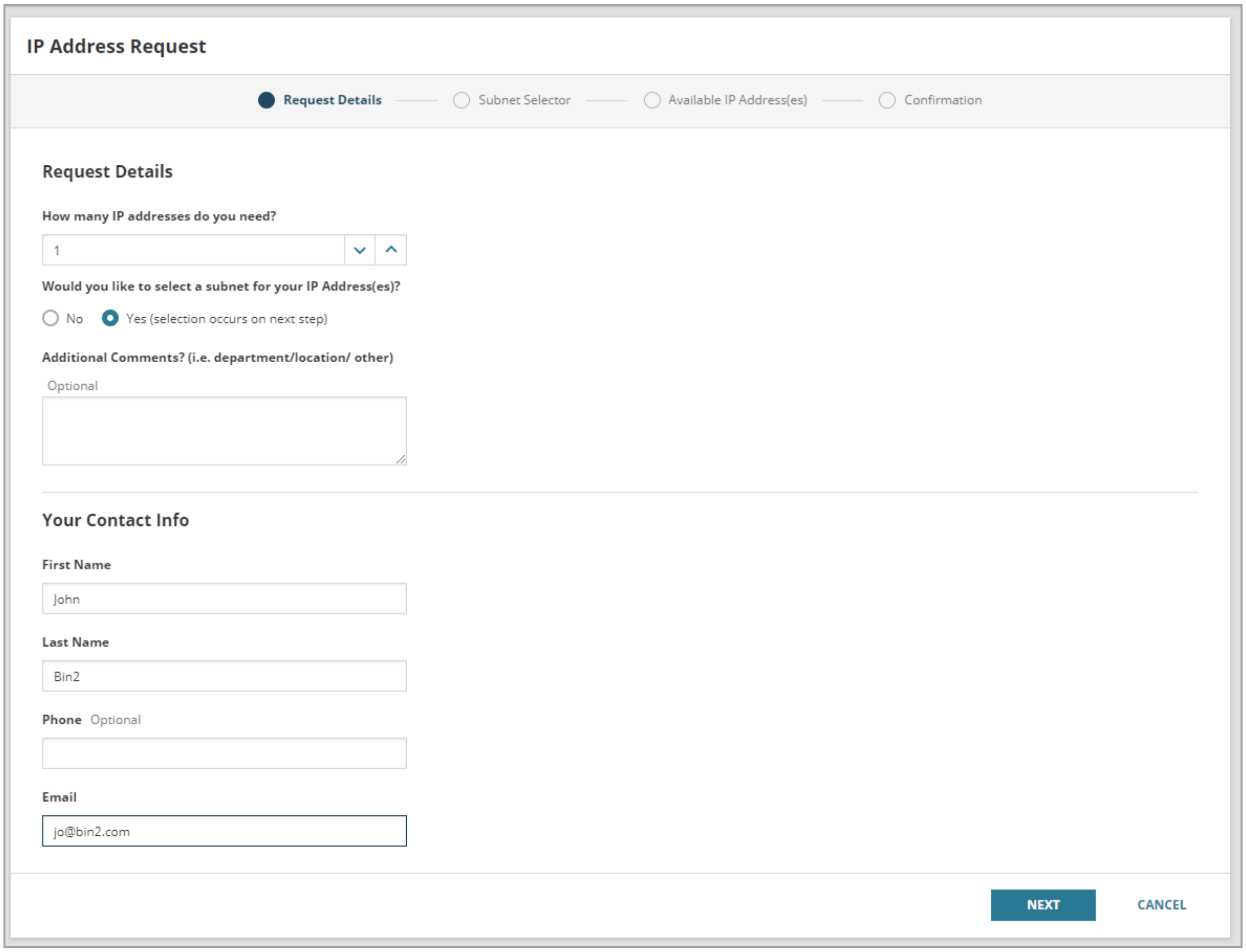
   Within the IPAM, an alert is created and displayed on the All Active Alerts page in the SolarWinds Web Console. For information on processing the request, see Process IP request alerts.

Request an IP address with IPAM access

If you have access to the SolarWinds Web Console, you can request IP addresses as described below.

The pages and fields displayed depend upon your IPAM permissions. The screenshots shown below are for a user with full access.

1. From the SolarWinds Web Console, go to My Dashboard > IP Addresses > Request IP Address.



IP Address Request

● Request Details — ○ Subnet Selector — ○ Available IP Address(es) — ○ Confirmation

Request Details

How many IP addresses do you need?

1

Would you like to select a subnet for your IP Address(es)?

○ No ● Yes (selection occurs on next step)

Additional Comments? (i.e. department/location/ other)

Optional

Your Contact Info

First Name

John

Last Name

Bin2

Phone Optional

Email

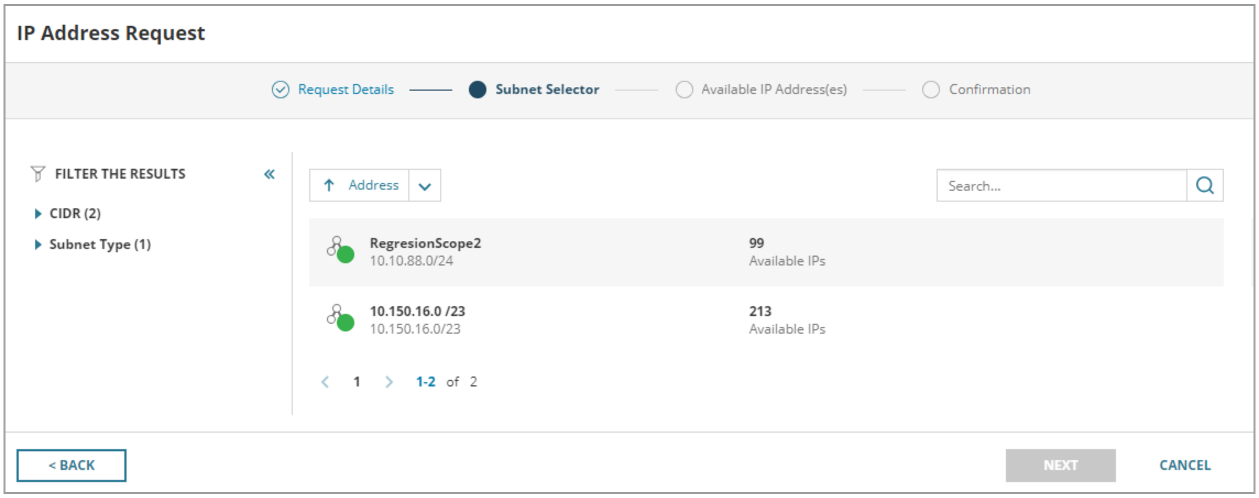
jo@bin2.com

2. Enter the number of IP addresses required.
3. If you want to select the subnet for your IP address(es), Click Yes. This option is only available if your IPAM role provides the appropriate permissions.
4. (Optional) Enter any comments you want to accompany this request.
5. Enter your contact information.

> ⓘ All fields except those marked as Optional must be completed.

6. Click Next.
   - If you selected No in Step 3, a message is displayed confirming your request, and an alert is displayed on the Active alerts page.
   - If you selected Yes in Step 3, the Subnet Selector page is displayed.

     Only subnets where there are sufficient IP addresses for the request are displayed.



IP Address Request

Request Details — Subnet Selector — Available IP Address(es) — Confirmation

FILTER THE RESULTS «

- CIDR (2)
- Subnet Type (1)

↑ Address ⌄ Search...

RegresionScope2 10.10.88.0/24 — 99 Available IPs

10.150.16.0 /23 10.150.16.0/23 — 213 Available IPs

‹ 1 › 1-2 of 2

< BACK NEXT CANCEL

7. Select the subnet to use, and click Next.
8. The Available IP Address(es) page is displayed. The first available IP addresses in the selected subnet are displayed.
9. If appropriate, enter the host names and MAC addresses for the reserved IP addresses.
10. Click Reserve Address(es).

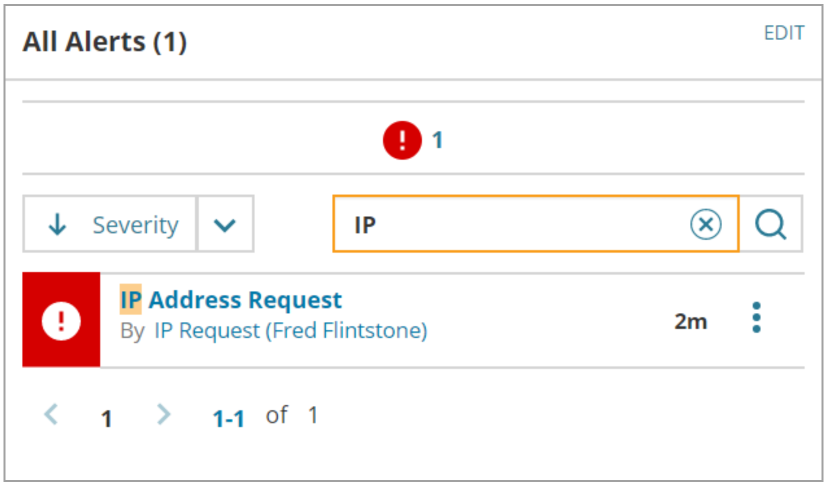
    A confirmation message is displayed to say that the request has been sent to the administrator.

    An alert is created, that will be displayed on the All Active Alerts page in the SolarWinds Web Console.

    For information on processing the request, see Process IP request alerts.

Process IP address requests

When someone requests IP addresses, an alert appears in the Active Alerts widget on the SolarWinds Summary view.



All Alerts (1) EDIT

! 1

↓ Severity ⌄ IP ⓧ

IP Address Request
By IP Request (Fred Flintstone) 2m ⋮

‹ 1 › 1-1 of 1

Click the alert title to open the Active Alert Details page.

This page shows information specifically for this alert. The Requester Details widget shows contact details, including those created in the Requester Details fields, for the person who made the request.

The alert should be acknowledged by clicking Acknowledge in the alert Status Overview widget. For more information on SolarWinds alerts, see Use alerts to monitor your environment with the IPAM.

Use the IP Address Request widget to process the request:

1. If the request does not specify a subnet, or you want to allocate IP addresses from a different subnet:
    a. Click Select Subnet in the IP Address Request(s) widget.
    b. Select the subnet on which you want to allocate IP addresses for this request. Only subnets containing sufficient addresses are displayed.
2. To deny individual IP address requests, click the Status icon to show ✖.
3. To add or change the Hostname or MAC Address or enter a value for a custom property assigned to the IP address, click the pencil icon and edit the appropriate fields on the pop-up window.
4. Click Process Request.
5. Enter any relevant comment to be emailed to the requester.
6. Click Reserve IPAM Only.

The IP addresses are now reserved in IPAM and can be seen on the IP Address View of the Manage Subnets & IP Addresses page.

To deny an entire IP request

Click Deny Request. You can optionally include a comment to be emailed to the requester.

The IPAM - All Created IP Requests report

A report showing all IP requests is available. This shows request date, number of addresses, the name of the user who made the request, and other details.

1. Go to Reports > All Reports.
2. Select IPAM Reports > IPAM - All Created IP Requests.

IP Request Settings

This page enables you to add administrators to be notified when IPs are requested, set up content in the request and notification emails, and add additional mandatory and optional fields to the IP request page.

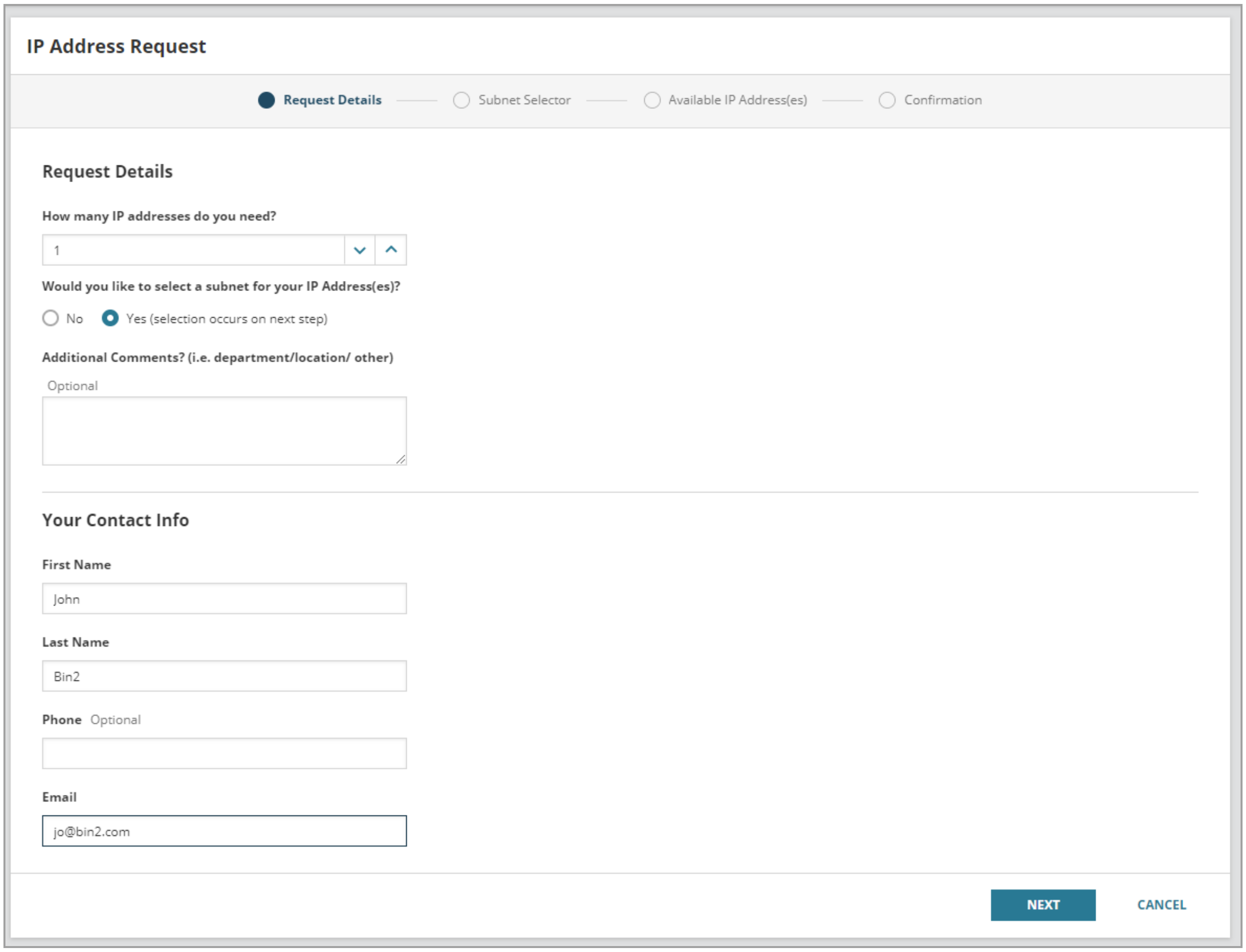
1. Navigate to Settings > All Settings > IPAM Settings > IPAM Request Settings.
2. Edit the settings are required.

IP Request form access settings	The settings, enable the administrator to set the security option for IP requests. For information, see The IP Request form access settings.
Requester Details fields	ⓘ These fields are displayed in addition to the mandatory First Name, Last Name, Phone and Email in the Your Contact Info section on the requester's IP Address Request page. a. Click Add New field, enter the field name and click Add. b. Check the Required box if this field must be completed by the requester.
Basic fields settings	Check the Required boxes if you want requesters who select a subnet to supply a Host Name and/or MAC address for each IP request.
Custom Properties	Custom properties set up for IPAM Nodes are displayed here. You can specify whether these properties are required or optional. You can also add, delete or edit custom properties by clicking Manage Custom Properties. See Custom properties in the IPAM for more information on Custom Properties.
Notification Settings	These fields enable you to specify: • The email addresses for administrators to be notified when IP addresses are requested • The signature text for the email notification sent to the administrator when a request is made • The signature text for emails sent to the requester when a request is processed or denied
Subnet Settings	Here you can specify whether scopes are to be included in subnet lists.

3. Click Save Changes.

Request an IP address with IPAM access

1. From the SolarWinds Web Console, go to My Dashboard > IP Addresses > Request IP Address.


● Request Details ○ Subnet Selector ○ Available IP Address(es) ○ Confirmation
NEXT
CANCEL

IP Address Request

Request Details

How many IP addresses do you need?

1

Would you like to select a subnet for your IP Address(es)?

○ No ● Yes (selection occurs on next step)

Additional Comments? (i.e. department/location/ other)

Optional

Your Contact Info

First Name

John

Last Name

Bin2

Phone Optional

Email

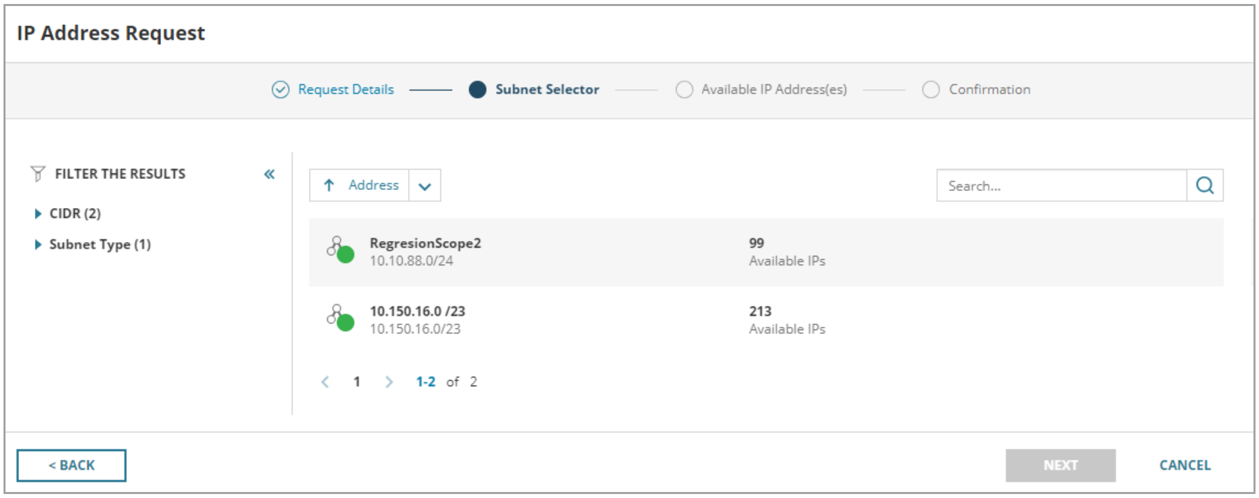
jo@bin2.com

2. Enter the number of IP addresses required.
3. If you want to select the subnet for your IP address(es), Click Yes.
4. (Optional) Enter any comments you want to accompany this request.
5. Enter your contact information.

> ⓘ All fields except those marked as Optional must be completed.

6. Click Next.
   - If you selected No in Step 3, a message is displayed confirming your request, and an alert is displayed on the Active alerts page.
   - If you selected Yes in Step 3, the Subnet Selector page is displayed.

     Only subnets where there are sufficient IP addresses for the request are displayed.



RegresionScope2 10.10.88.0/24	99 Available IPs
10.150.16.0 /23 10.150.16.0/23	213 Available IPs

7. Select the subnet to use, and click Next.
8. The Available IP Address(es) page is displayed. The first available IP addresses in the selected subnet are displayed.
9. If appropriate, enter the host names and MAC addresses for the reserved IP addresses.
10. Click Reserve Address(es).

    A confirmation message is displayed to say that the request has been sent to the administrator.

    An alert is created, that will be displayed on the All Active Alerts page in the SolarWinds Web Console.

    For information on processing the request, see Process IP request alerts.

Manage subnets in IPAM

Subnet creation and management are primary functions of IPAM.

SolarWinds recommends a maximum of around 125,000 subnets to avoid performance degradation. Using CIDR = 24, this allows for a total of around three million IP addresses.

This section includes the following topics:

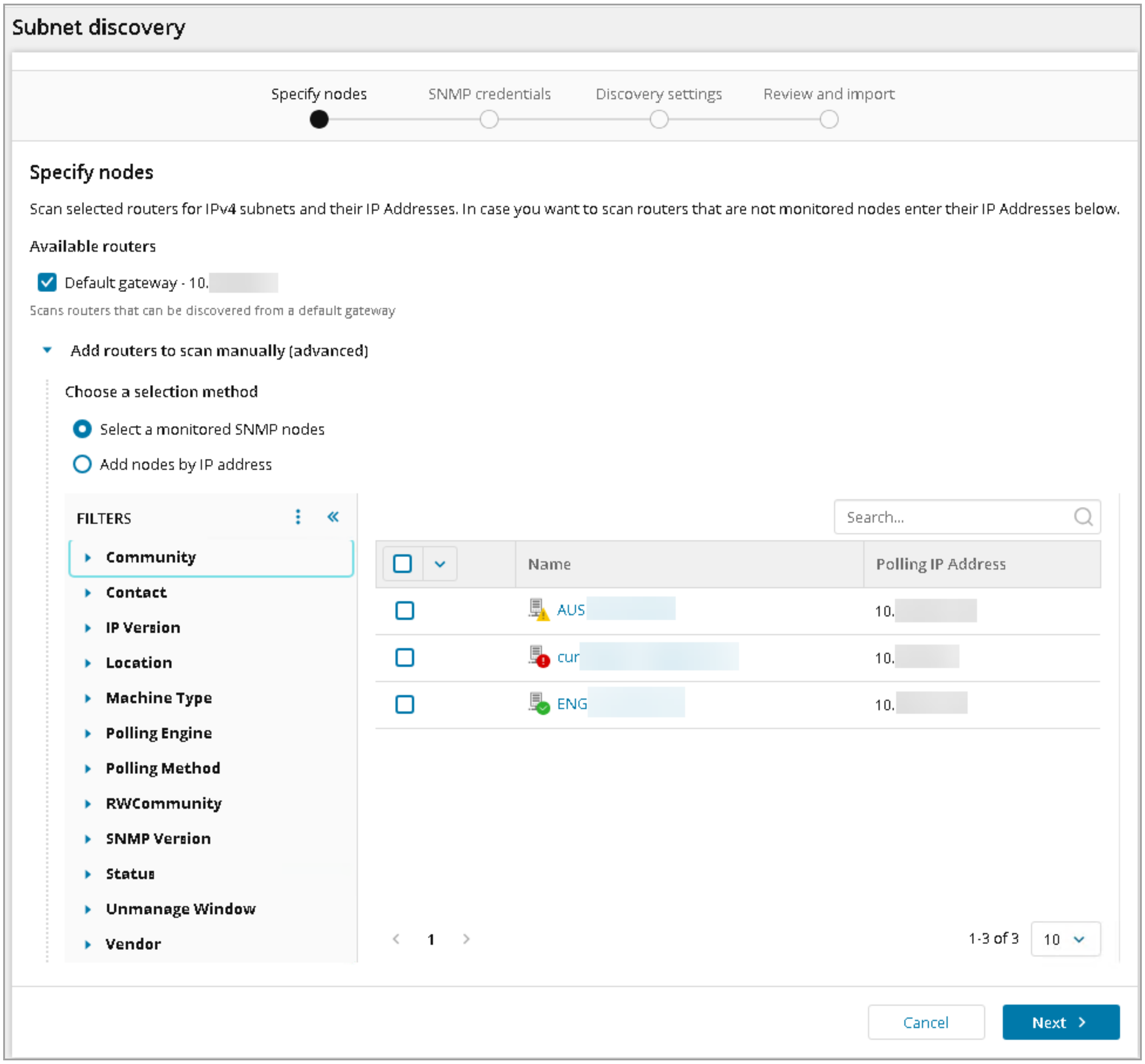
- Add IPv4 subnets and IP addresses
- Create subnets
- Edit subnets
- Bulk Add Subnets
- Export subnets
- IPAM Subnet Allocation wizard

Add IPv4 subnets and IP addresses

The Subnet Discovery wizard scans selected routers for IPv4 subnets and their IP Addresses and imports them into IPAM. The wizard eliminates the need for manual entry or the importing of IP Address spreadsheets.

1. Go to Settings > All Settings > IPAM Settings > Add Subnets & IP Addresses.
2. Select Discover routers & poll subnets and IP addresses from them, and click Next.

   The Subnet Discover wizard is displayed.



Subnet discovery

Specify nodes

Scan selected routers for IPv4 subnets and their IP Addresses. In case you want to scan routers that are not monitored nodes enter their IP Addresses below.

Available routers

☑ Default gateway - 10.[redacted]

Scans routers that can be discovered from a default gateway

Add routers to scan manually (advanced)

Choose a selection method

● Select a monitored SNMP nodes

○ Add nodes by IP address

□	Name	Polling IP Address
□	AUS[redacted]	10.[redacted]
□	cur[redacted]	10.[redacted]
□	ENG[redacted]	10.[redacted]

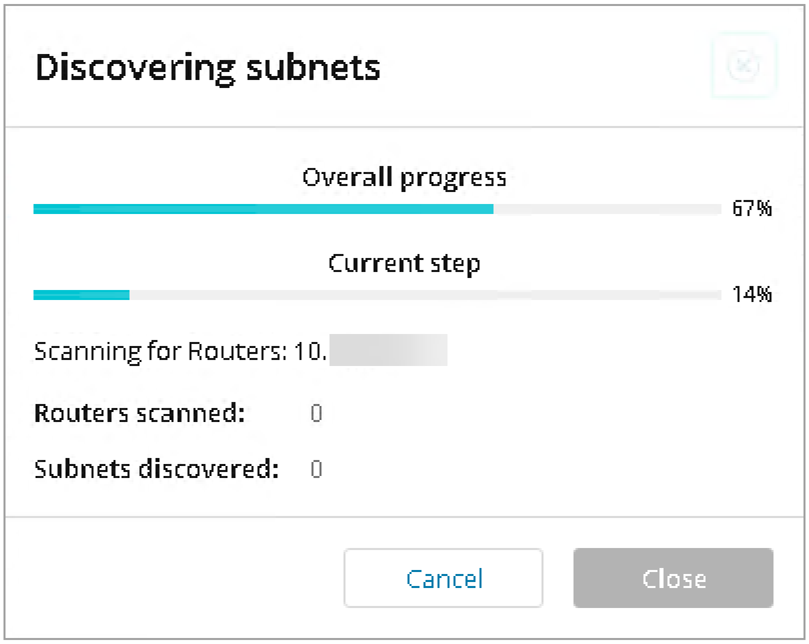
3. Select the nodes to scan. You can:

   - Accept the Default Gateway (Checked by default).
   - Select from the list of monitored SNMP nodes.
   - Manually add routers. To scan routers that are not monitored nodes, click Add nodes by IP Address, and add their IP addresses in the text box.

   Click Next.

4. If you need to add new credentials, click Add Credential, or click an existing credential. Click Next. For information on adding credentials, see Add SNMP credentials.

5. Adjust the Discovery Settings sliders for Hop Count and SNMP Timeouts. IPAM scans the default gateway and any other selected routers within the range of hops you determine. Click Discover subnets. The Discovering subnets progress bar is displayed.



Discovering subnets

Overall progress 67%

Current step 14%

Scanning for Routers: 10.[redacted]

Routers scanned: 0

Subnets discovered: 0

6. Select the IP addresses you want to import on the Subnet Discovery Review and Import page. Click Import.

How IPAM discovers IP addresses

IPAM uses device routing tables to poll the subnets.

The following OIDs are used during discovery and device polling:

Name	OID
IpForwarding	1.3.6.1.2.1.4.1
IpRouteDest	1.3.6.1.2.1.4.21.1.1
IpRouteMask	1.3.6.1.2.1.4.21.1.11.
IpCidrRouteDest	1.3.6.1.2.1.4.24.4.1.1.
IpCidrRouteMask	1.3.6.1.2.1.4.24.4.1.2
ipRouteType	1.3.6.1.2.1.4.21.1.8
NexthopAddress	1.3.6.1.2.1.4.21.1.7

Create subnets

Create subnets within selected subnets, supernets, and groups directly from the Manage Subnets & IP Addresses page.

> ⓘ You can also add multiple subnets using the Bulk Add Subnets.

1. Go to My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Select the network, group, or supernet to which you want to add a subnet.
3. Click Add > Subnet.
4. > ⓘ Click Add > Subnet Allocation wizard instead to create subnets within a designated supernet based on subnet size. See IPAM Subnet Allocation Wizard for more information.
5. Enter a subnet name. If you leave this field empty, IPAM automatically generates a name based on the subnet address and CIDR prefix length provided.
6. Provide a subnet address and a CIDR prefix length for the subnet.

   > ⓘ See IPAM concepts and terminology for more information about CIDR and subnet addressing.
7. (Optional) provide a description, VLAN ID, or location for the subnet.
8. If you have defined custom properties for subnets, or want to create them, you can do so here.
9. If you do not want IPAM to automatically scan this subnet for changes, select Disable Automatic Scanning.
10. Select the scan interval, or use the default period of 4 hours.
11. For information on using neighbor scanning to retrieve information on currently unresponsive devices within this subnet, see Neighbor scanning in IPAM
12. For information on setting a transient period for IP addresses in this subnet, see Configure subnet scan settings manually.
13. After you have configured the subnet, click Save.

You can drag and drop subnets into other groups and supernets to organize your network.

> ⓘ You cannot move subnets between Hierarchy groups.

Edit subnets

Use the Edit Subnet Properties box to edit the properties of a subnet, add custom information, add custom URLs, disable automatic scanning, change the scan interval, and customize user roles for the subnet.

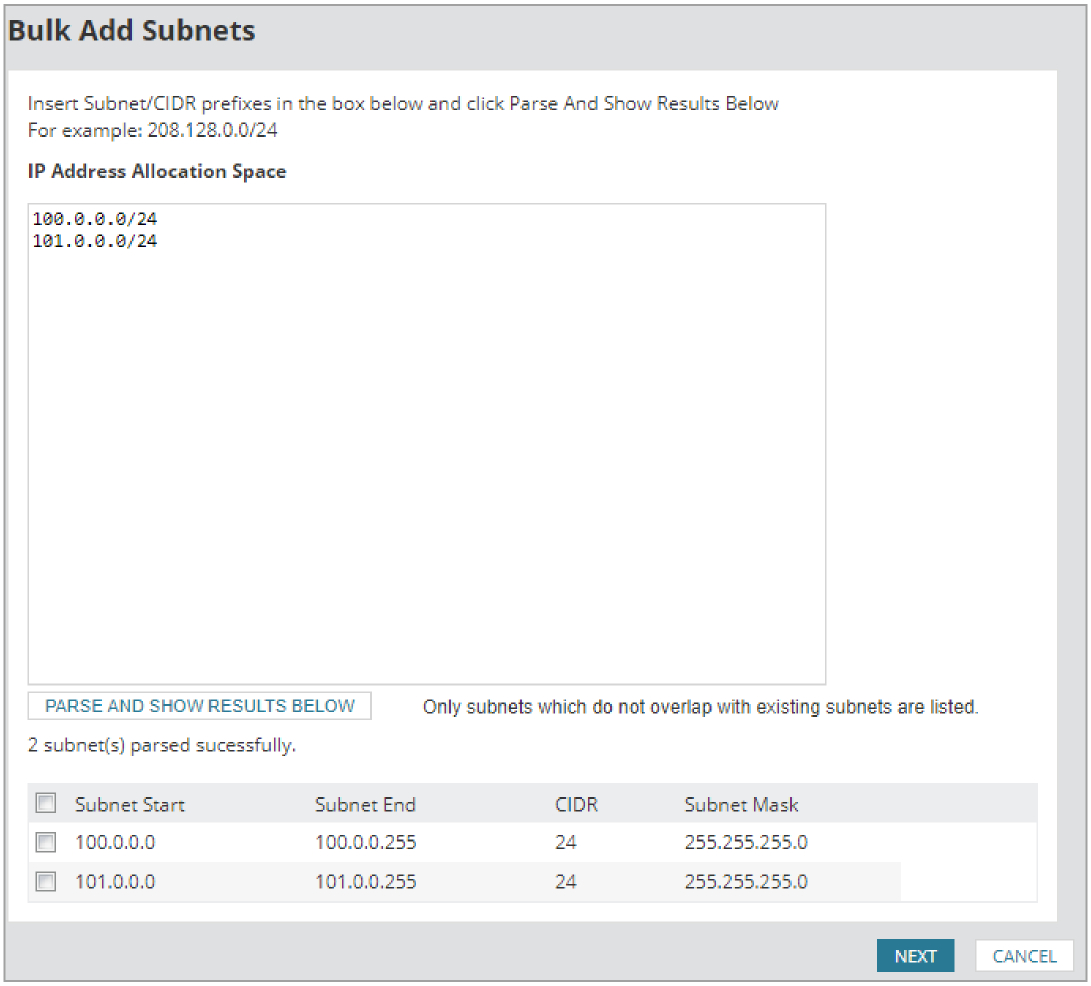
ⓘ The Edit Subnet properties box can also be accessed from the Scan Job Status window.

1. Click My Dashboards > IP Address Manager > Manage Subnets & IP Addresses.
2. Click the subnet you want to edit.
3. Click Properties.
4. Edit the subnet name and the CIDR prefix length for your subnet.
5. Edit the description, VLAN ID, or location for your subnet.
6. Edit the custom fields, server details, automatic scanning, transient period and account roles for this subnet if required.
7. Click Save after you have configured your subnet.

Bulk Add Subnets

The Bulk Add Subnets page enables you to manually enter a list of multiple subnets in one action.

1. Go to My Dashboards >IP Addresses > Manage Subnets & Addresses.
2. Select Import > Bulk Add Subnets.



Bulk Add Subnets

Insert Subnet/CIDR prefixes in the box below and click Parse And Show Results Below
For example: 208.128.0.0/24

IP Address Allocation Space

```
100.0.0.0/24
101.0.0.0/24
```

Only subnets which do not overlap with existing subnets are listed.

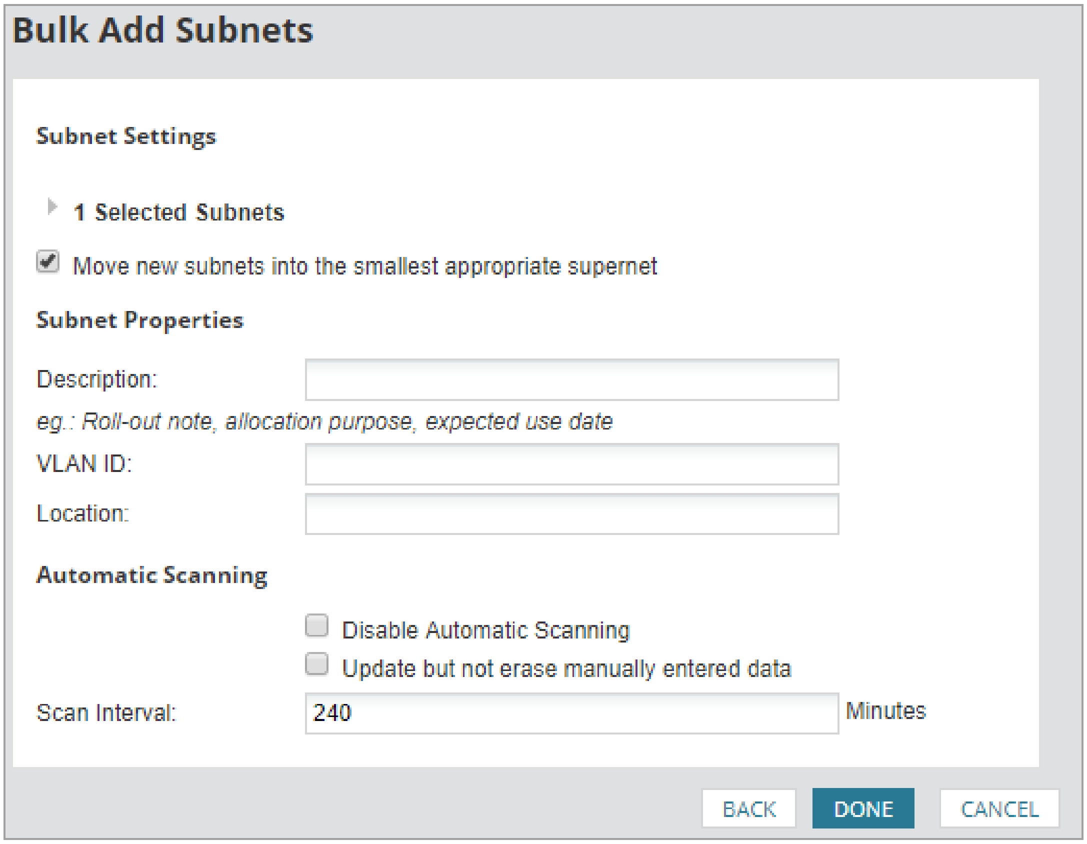
2 subnet(s) parsed sucessfully.

□	Subnet Start	Subnet End	CIDR	Subnet Mask
□	100.0.0.0	100.0.0.255	24	255.255.255.0
□	101.0.0.0	101.0.0.255	24	255.255.255.0

3. Enter the subnet/CIDRs into the IP Address Allocation Space.
4. Click Parse and show results below.

   The subnets are parsed, verified and listed showing the subnet start, send and mask.

5. Select the subnets to be added and click Next.



Bulk Add Subnets

Subnet Settings

1 Selected Subnets

☑ Move new subnets into the smallest appropriate supernet

Subnet Properties

Description:

eg.: Roll-out note, allocation purpose, expected use date

VLAN ID:

Location:

Automatic Scanning

□ Disable Automatic Scanning

□ Update but not erase manually entered data

Scan Interval: 240 Minutes

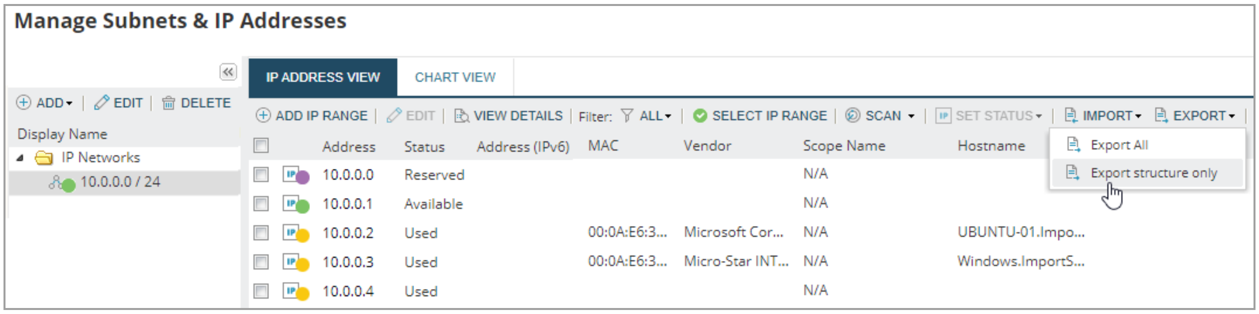
6. (Optional) Enter subnet details.
7. Click Done.
8. The Manage Subnets & IP Addresses page is redisplayed showing the subnets that were added.

Export subnets

You can export details of your entire IPAM network or selected objects within the network as spreadsheets. You can also choose to export just the structure.

> Due to limitations with the .xls format, it is only possible to export Excel files where:
>
> - IPAM 2020.2.1 and later: CIDR = 13 and higher (up to 524,288 addresses)
> - IPAM 2020.2 and earlier: CIDR = 17 and higher (up to 32,768 addresses)

1. Navigate to the Manage Subnets & IP Addresses page.
2. Select the objects to be exported. If you do not select anything, the entire network will be exported.



Manage Subnets & IP Addresses

□	Address	Status	Address (IPv6)	MAC	Vendor	Scope Name	Hostname
□	10.0.0.0	Reserved				N/A	
□	10.0.0.1	Available				N/A	
□	10.0.0.2	Used		00:0A:E6:3...	Microsoft Cor...	N/A	UBUNTU-01.Impo...
□	10.0.0.3	Used		00:0A:E6:3...	Micro-Star INT...	N/A	Windows.ImportS...
□	10.0.0.4	Used				N/A	

3. Click Export All.

> ⓘ To export only the structure, click Export structure only, and skip step 6 below.

4. Select the columns you want to export as the structure spreadsheet, and click Next.

   The first six columns (Id, Address, CIDR, Type, Display Name, and Parent Id) are mandatory.

5. Select the columns you want to export as the subnet spreadsheet(s), and click Next.

   Only the IP Address column is mandatory.

6. Select whether you want to export the data as .xls or .csv files, and click Export.
7. Enter a name for the zip file to be created or accept the default, and click Save.

   The zip file will consist of a structure spreadsheet and a sub-directory of subnet spreadsheets.

IPAM Subnet Allocation wizard

The Subnet Allocation Wizard provides a method to specify supernet and subnet sizes that can automatically be allocated.

- For an example of using the wizard to create subnets, see Create subnets.
- For an example of using the wizard to organize an IP address space into IPAM subnets, see Organize an IP address space into subnets.

Manage supernets in IPAM

Supernets are useful organizational tools for managing your network, and help bind multiple networks or subnets into one network with a single CIDR prefix, decreasing the size of routing tables and saving valuable memory and CPU cycles on routers.

The routing prefix of a supernet is aggregated from the prefixes of given networks or subnets and it must be smaller or the same as smallest component network prefix. Many supernet calculators are available online such as the Supernet Calculator (external link).

Create supernets

Create a supernet for organizing your network components.

1. Click IP Address Manager > Manage Subnets & IP Addresses.
2. Select the network, supernet, or group to which you want to add the supernet.
3. Click Add > Supernet.
4. Enter a name for your subnet.
5. Enter the supernet address and CIDR prefix length.
6. (Optional) provide a description for the supernet.
7. If you have defined custom properties, provide values.
8. After you have configured the supernet, click Save.

You can drag and drop the supernet into other groups and supernets to organize your network as required.

Edit supernets

To edit the properties of a supernet:

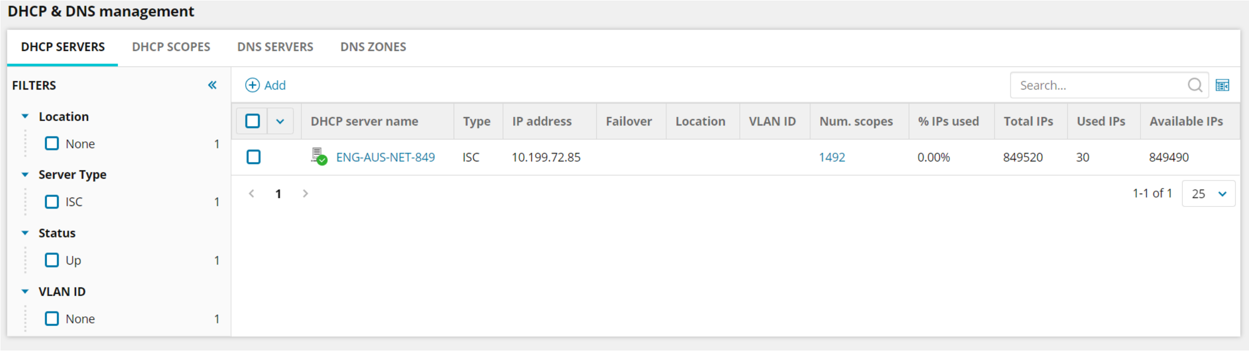
1. Click My Dashboards > IP Address Manager > Manage Subnets & IP Addresses.
2. Click the supernet you want to edit.

3. Click Properties.
4. Enter the supernet name and the CIDR prefix length.
5. (Optional) Enter a description for your supernet.
6. If you have defined custom properties for supernets, edit the values.
7. After you have configured your supernet, click Save.

DHCP and DNS Management views

The 2020.2 release of the IPAM IP Address Manager introduces an updated DHCP & DNS Management view, enabling dynamic filtering, improved workflows, and cleaner, refreshed layouts.

> ⚠ Internet Explorer is not supported by the new DHCP & DNS Management view. SolarWinds recommends using a different browser (such as Chrome or Firefox) for the best user experience.



Location
□ None 1

Server Type
□ ISC 1

Status
□ Up 1

VLAN ID
□ None 1

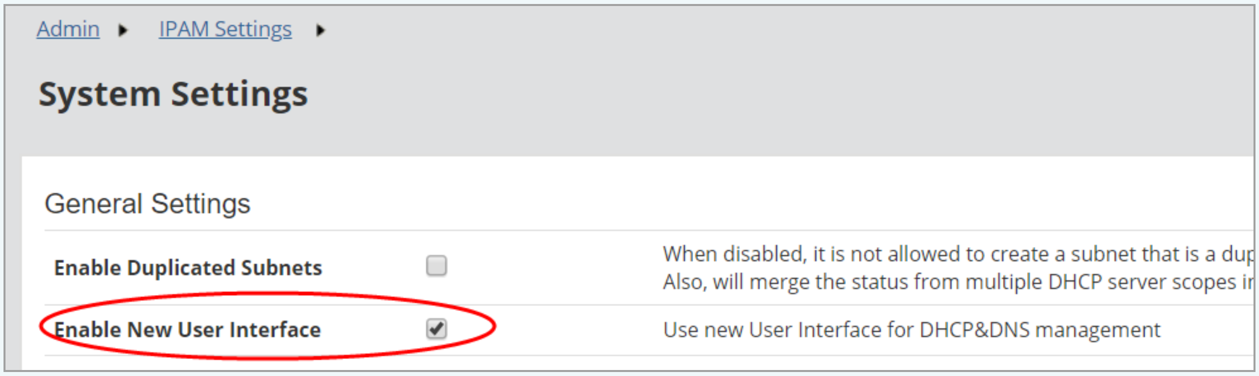
□	DHCP server name	Type	IP address	Failover	Location	VLAN ID	Num. scopes	% IPs used	Total IPs	Used IPs	Available IPs
□	ENG-AUS-NET-849	ISC	10.199.72.85				1492	0.00%	849520	30	849490

Switch between versions

The new version of the DHCP & DNS Management view is displayed by default.

If you prefer to use the previous version of the DHCP & DNS Management view, you can easily toggle between the new and legacy views.

1. From the navigation menu, go to Settings > All Settings > IPAM Settings.
2. In the Settings section on the left, click System Settings.
3. On the System Settings page, uncheck the Enable New User Interface box to use the legacy version. To return to the new version at any time, check this box.



Admin ▸ IPAM Settings ▸

System Settings

General Settings

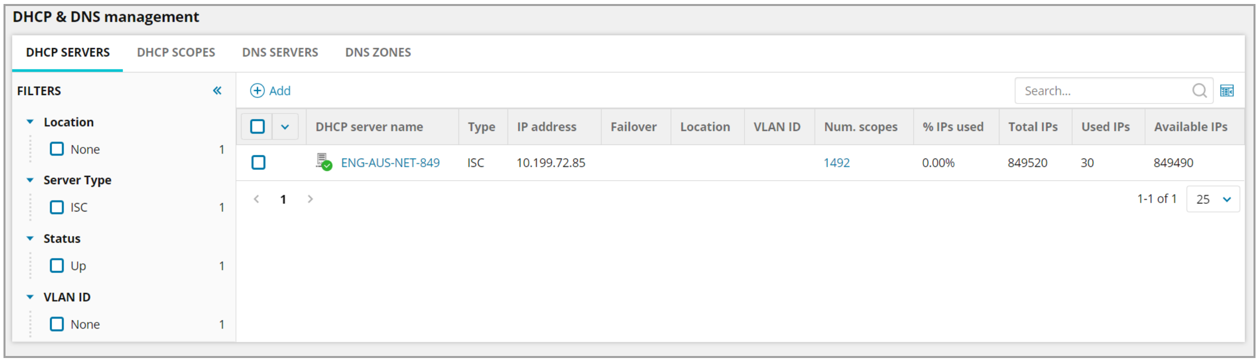
Enable Duplicated Subnets	□	When disabled, it is not allowed to create a subnet that is a dup Also, will merge the status from multiple DHCP server scopes ir
Enable New User Interface	☑	Use new User Interface for DHCP&DNS management

See also:

The IPAM DHCP and DNS Management view

With the 2020.2 release of IPAM, an improved, updated version of the DHCP & DNS Management page is displayed by default.

This page allows you to navigate through various tabs to manage your DHCP servers and scopes, and DNS servers and zones.



DHCP & DNS management

Location
□ None 1

Server Type
□ ISC 1

Status
□ Up 1

VLAN ID
□ None 1

□	DHCP server name	Type	IP address	Failover	Location	VLAN ID	Num. scopes	% IPs used	Total IPs	Used IPs	Available IPs
□	ENG-AUS-NET-849	ISC	10.199.72.85				1492	0.00%	849520	30	849490

‹ 1 › 1-1 of 1 25

The DHCP & DNS Management page is divided into two panes.

The left pane provides filters (depending on the selected tab) that enable you to narrow down the items displayed. Expand each filter to show the categories within the filter type. Categories for which no items are displayed are hidden.

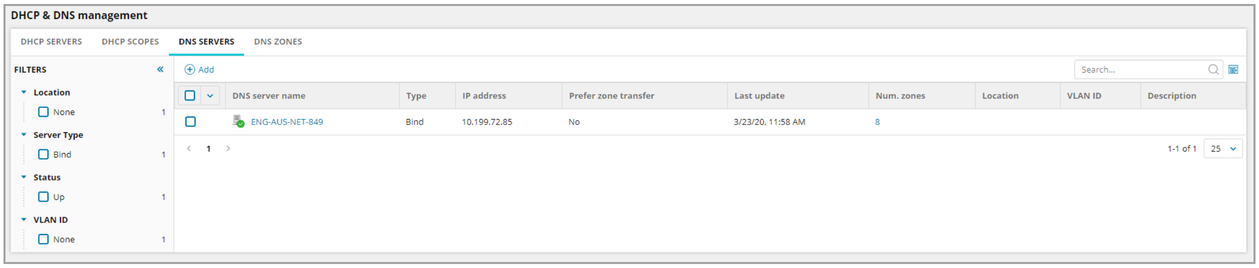
The right pane provides one of four views, selected by clicking the links on the menu bar:

- DHCP Servers
- DHCP Scopes
- DNS Servers
- DNS Zones

The columns displayed for these views can be edited by clicking the icon next to the search box. Select the columns to be displayed (and uncheck those to be hidden), and click Update Columns.

DHCP Servers

The DHCP Servers view displays a list of DHCP Servers currently being monitored in IPAM. These can be filtered by Location, Server Type, Status, and VLAN ID in the left column.

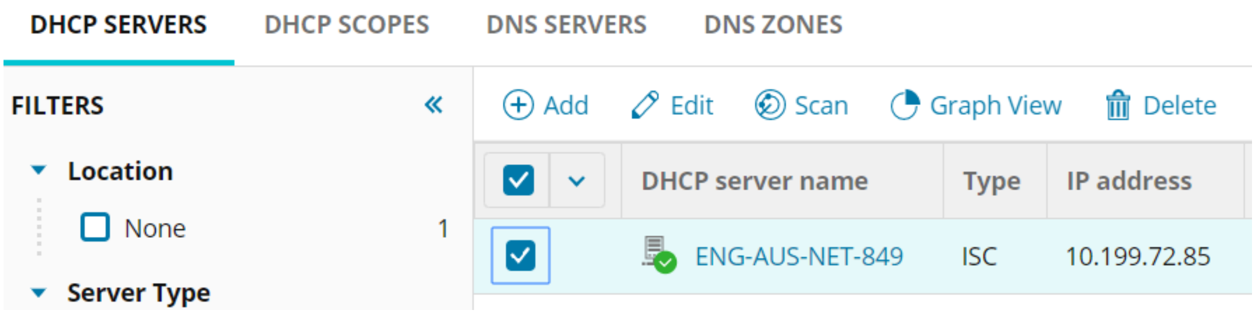


□	DNS server name	Type	IP address	Prefer zone transfer	Last update	Num. zones	Location	VLAN ID	Description
□	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	8			

Click on a server name to display the DHCP Server Details page.

Click Add to open the Add DHCP Server page for this server.

If you select a server, additional options are displayed:

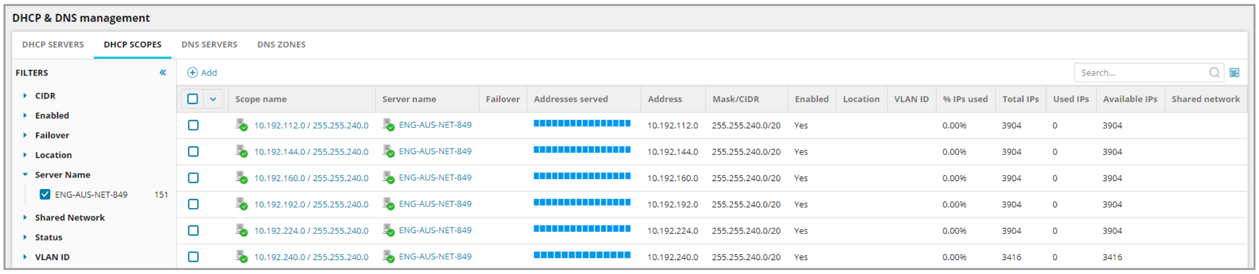


☑	DHCP server name	Type	IP address
☑	ENG-AUS-NET-849	ISC	10.199.72.85

For information on DHCP servers, see Monitor and manage DHCP servers.

DHCP Scopes

The DHCP Scopes view displays a list of DHCP scopes currently being monitored in IPAM. These can be filtered by CIDR, Enabled, Status, Failover, Location, Server name, Status and VLAN ID. Click on a scope name to display the IP Address view for this scope. Click on a Server name to display to display the DHCP Server Details page for the server.

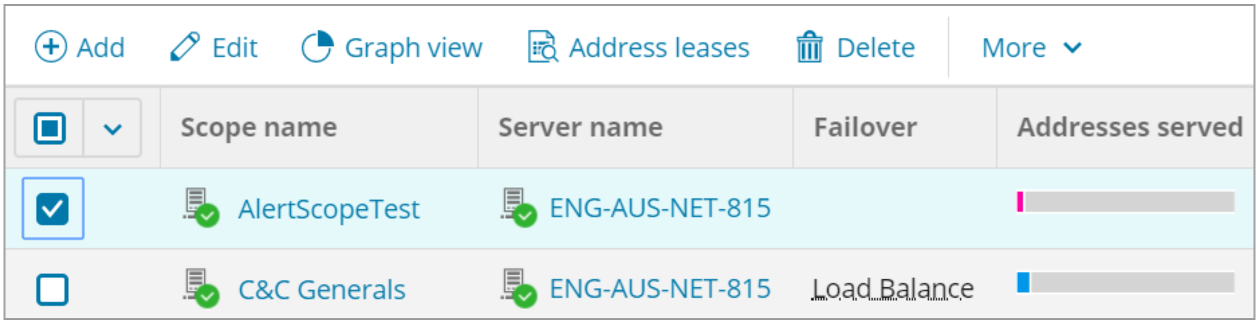


DHCP & DNS management

□	Scope name	Server name	Failover	Addresses served	Address	Mask/CIDR	Enabled	Location	VLAN ID	% IPs used	Total IPs	Used IPs	Available IPs	Shared network
□	10.192.112.0 / 255.255.240.0	ENG-AUS-NET-849			10.192.112.0	255.255.240.0/20	Yes			0.00%	3904	0	3904	
□	10.192.144.0 / 255.255.240.0	ENG-AUS-NET-849			10.192.144.0	255.255.240.0/20	Yes			0.00%	3904	0	3904	
□	10.192.160.0 / 255.255.240.0	ENG-AUS-NET-849			10.192.160.0	255.255.240.0/20	Yes			0.00%	3904	0	3904	
□	10.192.192.0 / 255.255.240.0	ENG-AUS-NET-849			10.192.192.0	255.255.240.0/20	Yes			0.00%	3904	0	3904	
□	10.192.224.0 / 255.255.240.0	ENG-AUS-NET-849			10.192.224.0	255.255.240.0/20	Yes			0.00%	3904	0	3904	
□	10.192.240.0 / 255.255.240.0	ENG-AUS-NET-849			10.192.240.0	255.255.240.0/20	Yes			0.00%	3416	0	3416	

Click Add to open the Add DHCP Scope page for this server.

If you select a scope, additional options are displayed.

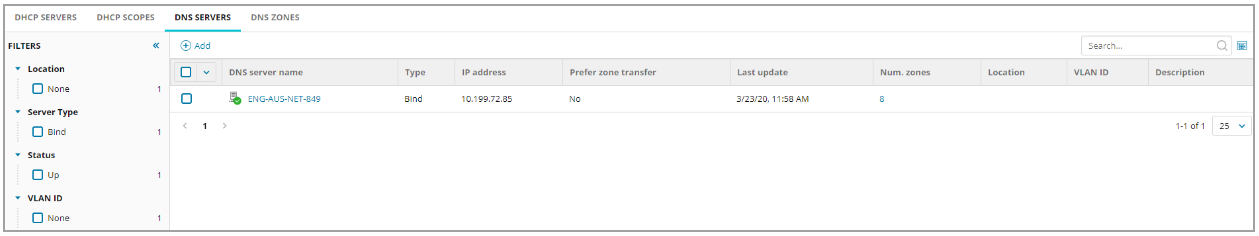


□	Scope name	Server name	Failover	Addresses served
☑	AlertScopeTest	ENG-AUS-NET-815		
□	C&C Generals	ENG-AUS-NET-815	Load Balance	

For information on DHCP scopes, see Create or edit a scope on a DHCP server.

DNS Servers

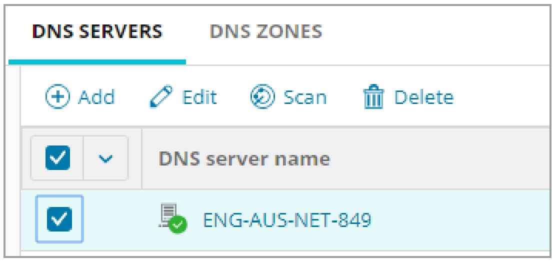
The DNS Servers view displays a list of DNS Servers currently being monitored in IPAM. These can be filtered by Location, Server Type, Status and VLAD ID. Click on the server name to open the DNS Zones tab showing the DNS zones for this server.



□	DNS server name	Type	IP address	Prefer zone transfer	Last update	Num. zones	Location	VLAN ID	Description
□	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	8			

Click Add to open the Add DNS server page.

If you select a server, the following additional options are displayed.

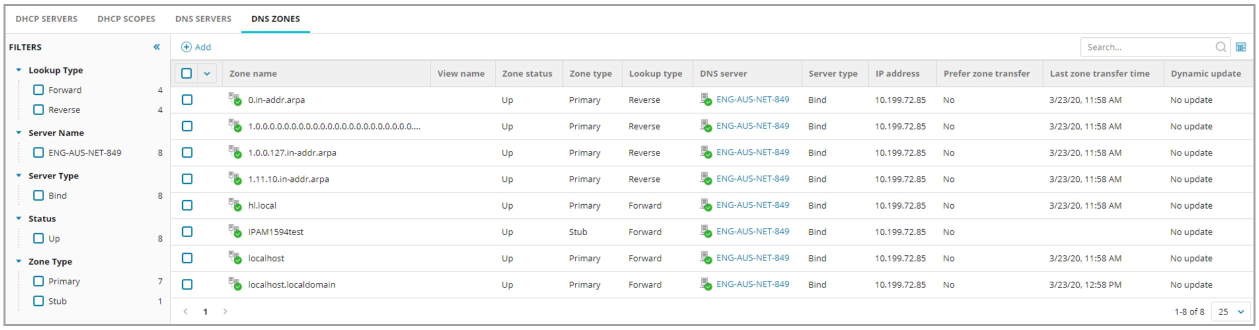


☑	DNS server name
☑	ENG-AUS-NET-849

For details on adding, editing and using DNS servers, see Monitor and Manage DNS servers.

DNS Zones

The DNS zones view displays a list of DNS zones currently being monitored in IPAM. These can be filtered by Lookup Type, Server Name, Location, Server Type, Status and Zone Type.



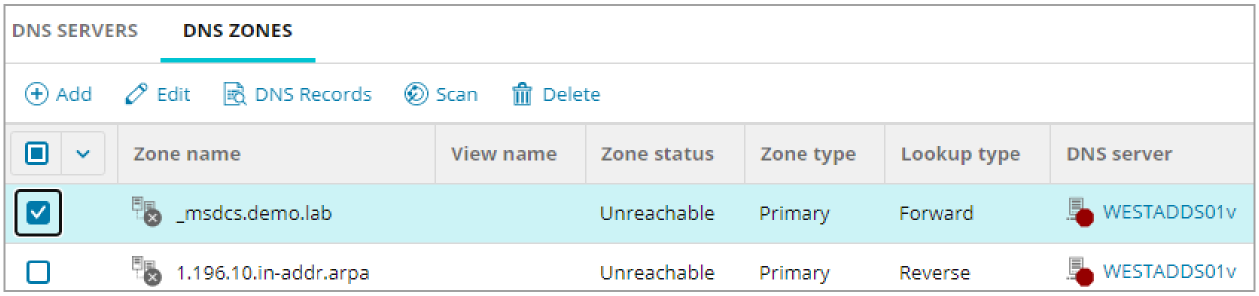
FILTERS	
Lookup Type	
□ Forward	4
□ Reverse	4
Server Name	
□ ENG-AUS-NET-849	8
Server Type	
□ Bind	8
Status	
□ Up	8
Zone Type	
□ Primary	7
□ Stub	1

□	Zone name	View name	Zone status	Zone type	Lookup type	DNS server	Server type	IP address	Prefer zone transfer	Last zone transfer time	Dynamic update
□	0.in-addr.arpa		Up	Primary	Reverse	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	No update
□	1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0....		Up	Primary	Reverse	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	No update
□	1.0.0.127.in-addr.arpa		Up	Primary	Reverse	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	No update
□	1.11.10.in-addr.arpa		Up	Primary	Reverse	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	No update
□	hl.local		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	No update
□	IPAM1594test		Up	Stub	Forward	ENG-AUS-NET-849	Bind	10.199.72.85	No		No update
□	localhost		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 11:58 AM	No update
□	localhost.localdomain		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85	No	3/23/20, 12:58 PM	No update

1-8 of 8 25

Click Add to open the Add a DNS zone.

If you select a DNS zone, additional options are displayed.



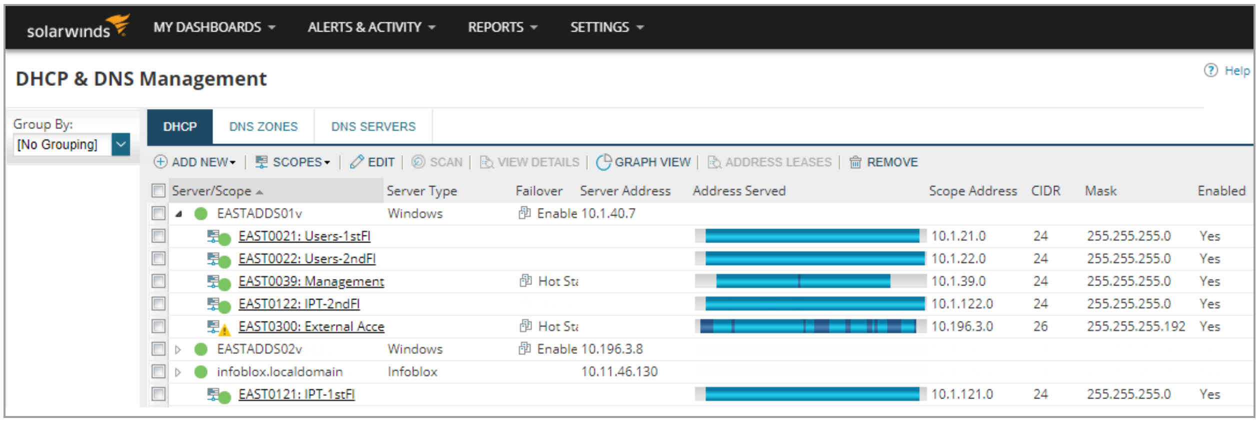
■	Zone name	View name	Zone status	Zone type	Lookup type	DNS server
☑	_msdcs.demo.lab		Unreachable	Primary	Forward	WESTADDS01v
□	1.196.10.in-addr.arpa		Unreachable	Primary	Reverse	WESTADDS01v

For information on using DNS zones, see Add a DNS zone and Edit a DNS zone.

The IPAM DHCP & DNS Management (Legacy) view

The legacy IPAM DHCP & DNS Management page allows you to navigate through tabs to manage your DNS and DHCP servers.

To toggle between new and legacy versions of the DHCP & DNS Management page, see Switch between versions.



□	Server/Scope	Server Type	Failover	Server Address	Address Served	Scope Address	CIDR	Mask	Enabled
□	EASTADDS01v	Windows	Enable	10.1.40.7					
□	EAST0021: Users-1stFl					10.1.21.0	24	255.255.255.0	Yes
□	EAST0022: Users-2ndFl					10.1.22.0	24	255.255.255.0	Yes
□	EAST0039: Management		Hot St			10.1.39.0	24	255.255.255.0	Yes
□	EAST0122: IPT-2ndFl					10.1.122.0	24	255.255.255.0	Yes
□	EAST0300: External Acce		Hot St			10.196.3.0	26	255.255.255.192	Yes
□	EASTADDS02v	Windows	Enable	10.196.3.8					
□	infoblox.localdomain	Infoblox		10.11.46.130					
□	EAST0121: IPT-1stFl					10.1.121.0	24	255.255.255.0	Yes

The DHCP & DNS Management page is divided into two panes.

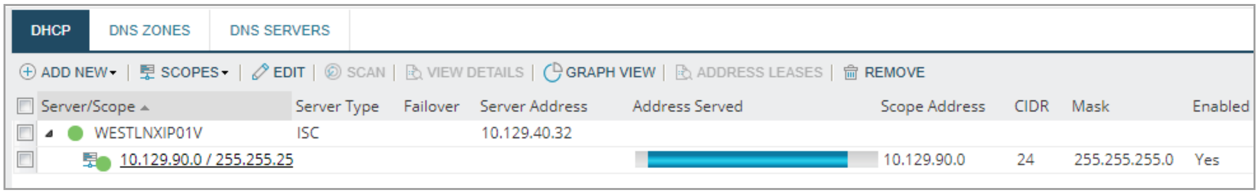
The left pane can be used to group and select the items displayed by catagories.

The right pane provides three tabs, providing the following views:

- DHCP tab
- DNS Zones tab
- DNS Servers tab

The columns in the DHCP, DNS Zones and DNS Servers views can be hidden or displayed by moving the cursor over any column heading, clicking on the down arrow that appears, selecting Add/Remove Columns, and selecting or deselecting the appropriate item. You can also drag and drop the columns into the order required in the DNS Zones and DNS Servers views. These changes will be retained for your login.

DHCP tab



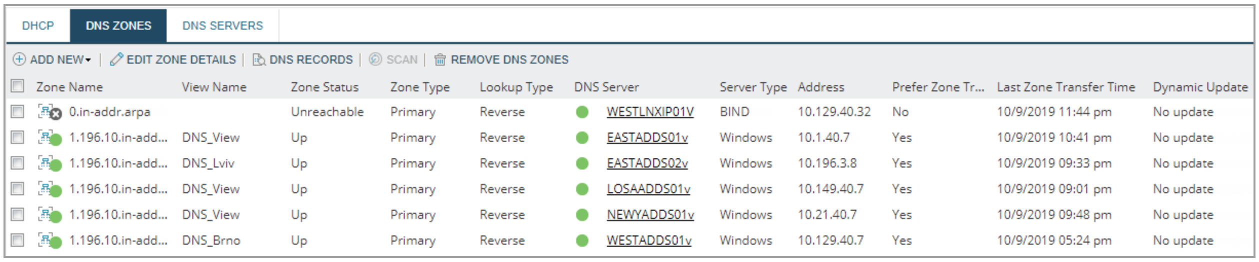
□	Server/Scope	Server Type	Failover	Server Address	Address Served	Scope Address	CIDR	Mask	Enabled
□	WESTLNXIP01V	ISC		10.129.40.32					
□	10.129.90.0 / 255.255.25					10.129.90.0	24	255.255.255.0	Yes

The DHCP Servers tab displays a list of all DHCP Servers that are monitored in IPAM. These can be grouped by server type, VLAD ID, server location or status, or by Scopes name or status.

For information on adding and editing DHCP servers, see Monitor and manage DHCP servers.

- Click the icon before a Server to display the scopes on this server.
- Click a scope to open the IP Address View details.

DNS Zones tab

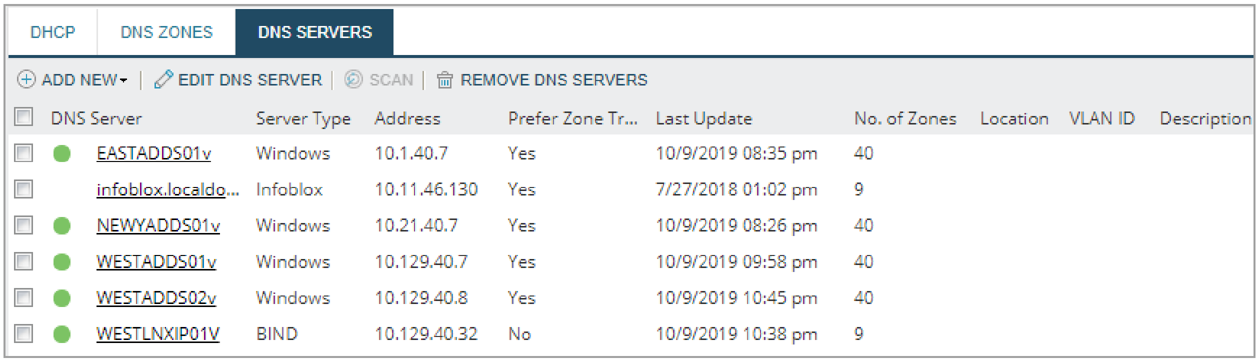


□	Zone Name	View Name	Zone Status	Zone Type	Lookup Type	DNS Server	Server Type	Address	Prefer Zone Tr...	Last Zone Transfer Time	Dynamic Update
□	0.in-addr.arpa		Unreachable	Primary	Reverse	● WESTLNXIP01V	BIND	10.129.40.32	No	10/9/2019 11:44 pm	No update
□	1.196.10.in-add...	DNS_View	Up	Primary	Reverse	● EASTADDS01v	Windows	10.1.40.7	Yes	10/9/2019 10:41 pm	No update
□	1.196.10.in-add...	DNS_Lviv	Up	Primary	Reverse	● EASTADDS02v	Windows	10.196.3.8	Yes	10/9/2019 09:33 pm	No update
□	1.196.10.in-add...	DNS_View	Up	Primary	Reverse	● LOSAADDS01v	Windows	10.149.40.7	Yes	10/9/2019 09:01 pm	No update
□	1.196.10.in-add...	DNS_View	Up	Primary	Reverse	● NEWYADDS01v	Windows	10.21.40.7	Yes	10/9/2019 09:48 pm	No update
□	1.196.10.in-add...	DNS_Brno	Up	Primary	Reverse	● WESTADDS01v	Windows	10.129.40.7	Yes	10/9/2019 05:24 pm	No update

The DNS Zones tab displays all monitored DNS Zones. These can be grouped by zones by server or status, or servers by status or server type.

For information on DNS zones, see Add a DNS zone and Edit a DNS zone.

DNS Servers Tab



□	DNS Server	Server Type	Address	Prefer Zone Tr...	Last Update	No. of Zones	Location	VLAN ID	Description
□	● EASTADDS01v	Windows	10.1.40.7	Yes	10/9/2019 08:35 pm	40			
□	infoblox.localdo...	Infoblox	10.11.46.130	Yes	7/27/2018 01:02 pm	9			
□	● NEWYADDS01v	Windows	10.21.40.7	Yes	10/9/2019 08:26 pm	40			
□	● WESTADDS01v	Windows	10.129.40.7	Yes	10/9/2019 09:58 pm	40			
□	● WESTADDS02v	Windows	10.129.40.8	Yes	10/9/2019 10:45 pm	40			
□	● WESTLNXIP01V	BIND	10.129.40.32	No	10/9/2019 10:38 pm	9			

The DNS Servers tab displays all monitored DNS Servers. These can be grouped by zones by server or status, or servers by status or server type.

For information on adding and editing DNS servers, see Monitor and manage DNS servers.

- Click a server to display the DNS Zones tab, grouped by Server.

Monitor and manage DHCP servers

IPAM integrates DHCP and DNS management with IP address management into one interface. You can manage Cisco, Infoblox, ISC and Microsoft DHCP servers.

> ⓘ Since Infoblox monitoring is read-only certain DHCP operations are unavailable. For further information see Monitor the Infoblox environment.

This section covers:

- Requirements for monitoring Cisco and ASA servers
- Manage and monitor ISC DHCP servers
- Add, edit, or remove a DHCP server to IPAM
- DHCP Impersonation
- Edit a DHCP Server
- Create or edit a scope on a DHCP server
    - Define scope options on a DHCP server
    - Configure split scopes on DHCP servers
    - Discovered Scopes
    - Remove a scope
- Set up and monitor Windows DHCP server failover
- Reserve an IP Address on a Windows DHCP server
- Troubleshooting DHCP and DNS connections in IPAM
- ARP table

Requirements for monitoring Cisco and ASA servers

To monitor Cisco and ASA DHCP servers in IPAM, the devices being added must support the following:

- Cisco devices commands:

```
- 'show running-config'

- 'show ip dhcp pool'

- 'show ip dhcp binding'
```

- ASA device commands:

```
-show dhcpd binding-show running-config dhcpd-show dhscpd statistics
```

```
    -show interface l inc interface l ip address
```

- Layer 3 switch or router
- IOS version 12.2(8)T or later
- Enable level 15

Manage and monitor ISC DHCP servers

Use ISC DHCP management and monitoring support to create, edit, or remove DHCP subnets directly and update servers automatically through the SolarWinds Web Console. You can also manage ISC DHCP subnet options, ranges, pools, and monitor ISC shared subnet utilization. Monitor server status and availability and IP address static assignments within groups.

> ⓘ Nested configurations are **not** supported.

The following settings and specifications are required for IPAM to access your ISC servers.

Base version for ISC	isc-dhcp-4.2.4-P1
Operating system	POSIX compliant Linux distributions

User access	• User account configured to enable remote telnet* or SSH access to ISC DHCP machine
	* The root account cannot be used in telnet. Also, a banner is required in telnet in the form:
	`"`
	`<empty line>`
	`Some customer telnet message`
	`"`
	• Read and write file access for users on the configuration files

<table>
<tr><td>CLI commands</td><td>• dhcpd --version
• grep
• echo $PATH_DHCPD_DB
• dhcpd -t -cf
• ps -w -A -o comm,pid,args | grep ^dhcpd –w (or) ps -A -o comm,pid,args | grep ^dhcp (or) ps -x -o comm,pid,args | grep ^dhcp
• [-f ""] && echo 'true'
• uname -mrs
• sha1sum (or) sha1 (or) digest -v -a sha1
• [-r ""] && echo 'true'
• [-w ""] && echo 'true'
• cat
• \cp -u -f -b -S.backup -p "" ""
• \rm -r -f ""
• mkdir</td></tr>
<tr><td>Configuration file</td><td>IPAM seeks the configuration file in one of the following paths:
• /etc/dhcpd.conf
• /etc/inet/dhcpd4.conf
• /etc/dhcp/dhcpd.conf
• /usr/local/etc/dhcpd.conf</td></tr>
<tr><td>Lease file</td><td>• /var/db/dhcpd.leases
• /var/lib/dhcpd/dhcpd.leases
• /var/lib/dhcp/dhcpd.leases
• /var/db/dhcpd/dhcpd.leases</td></tr>
<tr><td>Script file</td><td>• /etc/init.d/dhcpd
• /etc/init.d/dhcp
• /etc/rc.d/dhcpd
• /usr/local/etc/rc.d/isc-dhcpd
• /etc/init.d/isc-dhcp-server
• /usr/sbin/dhcpd</td></tr>
</table>

Configure an ISC DHCP server

On a new installation of ISC DHCP from a terminal prompt:

1. Enter the following command to install the DHCP server program, DHCPD:

   ```
   sudo apt-get install isc-dhcp-server
   ```

2. To change the default configuration, edit the file:

   ```
   /etc/dhcp3/dhcpd.conf
   ```

3. To specify the interfaces DHCPD listens to, edit:

   `/etc/default/isc-dhcp-server`.

   By default, DHCPD listens to `eth0`.

4. Assign a static IP to the interface that you use for DHCP.

   > ⓘ Verify that the ISC service is running so IPAM can communicate with your ISC DHCP server. After you edit the configuration file, restart the service.

To begin managing your ISC servers, they must first be added to IPAM. See Add DHCP servers to IPAM for more information.

Add, edit, or remove a DHCP server to IPAM

Add a DHCP server to IPAM to manage its scopes and IP address leases. A scope is a range of IP addresses that the DHCP server leases to clients on a subnet.

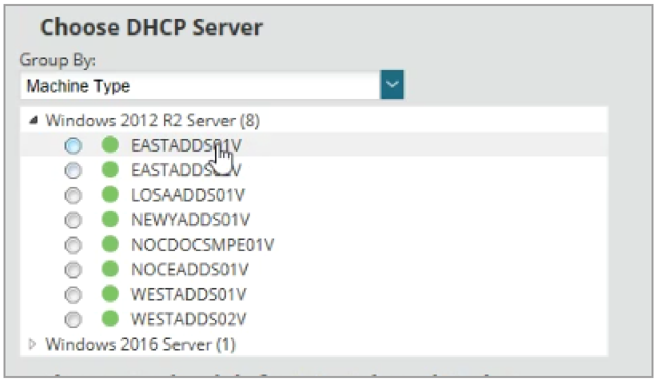
In this topic:

- Add a DHCP server
- Edit DHCP server properties
- Remove a DHCP server

Add a DHCP server

> ⓘ Before adding a DHCP server to IPAM, it must already exist as a node. Therefore, verify that you have completed the following tasks:
>
> - Discover devices using Active Directory domain controllers
> - Add discovered devices to SolarWinds IPAM

1. Click Settings > All Settings > IPAM Settings > Add DHCP server.
2. Select the server from the Choose DHCP Server drop-down menu. You can group servers by a variety of methods to make finding the required server easier.



Group By: Machine Type

3. Select a credential type, and either select the credential name to be used, or create a new credential.

> ⓘ To create a new credential, you will need a valid user name and password, plus an Enable password for the Enable Level for CISCO or ASA. For information on creating a new credential, see Manage credentials.

The account specified in the credential must exist on the DHCP server and be a member of one of the three following groups:

- DHCP Users
- DHCP Administrators
- Local Administrators

IPAM impersonates the specified account on the local computer in order to gain access.

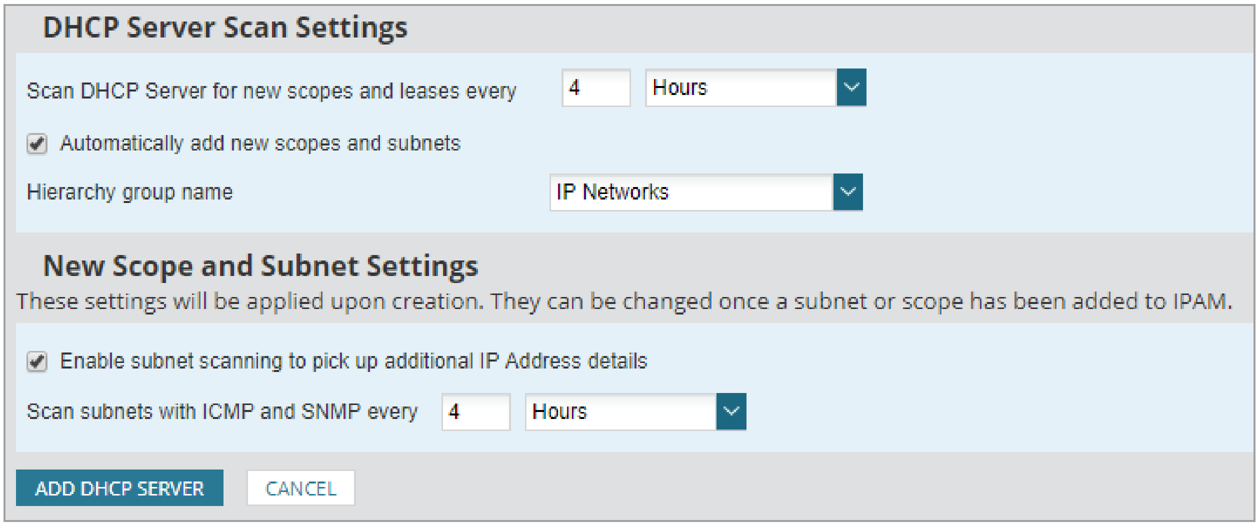
> ⓘ If the IPAM computer is not within the same domain as the DHCP server, the IPAM computer must have the identical account and password.

4. Click Test to verify the credential on the selected server.
5. Select your default DHCP Server Scan Settings, and click Add DHCP Server.
6. Select the scan interval. The default is set to four hours.
7. If you want to automatically add new scopes and subnets after scanning, check the box.
8. If you want IPAM to scan using ICMP and SNMP to obtain additional IP Address details, check the Enable subnet scanning box and select the scanning interval.
9. If you want to use or create an hierarchy group to which subnets discovered by this server are assigned, select the group name from the Hierarchy group name drop-down. If you leave this as IP Networks, all discovered subnets will be assigned to the IP Networks hierarchy group.

10. To create a new Hierarchy group, select New Hierarchy group name and enter the name for the group.

> ⓘ Hierarchy groups enable you to have overlapping IP addresses, which can happen if you have identical subnets in different locations monitored by different DHCP servers on the same network.

> ⓘ Hierarchy groups cannot be used for an Infoblox server, and the field is not available.



DHCP Server Scan Settings

Scan DHCP Server for new scopes and leases every: 4 Hours

☑ Automatically add new scopes and subnets

Hierarchy group name: IP Networks

New Scope and Subnet Settings

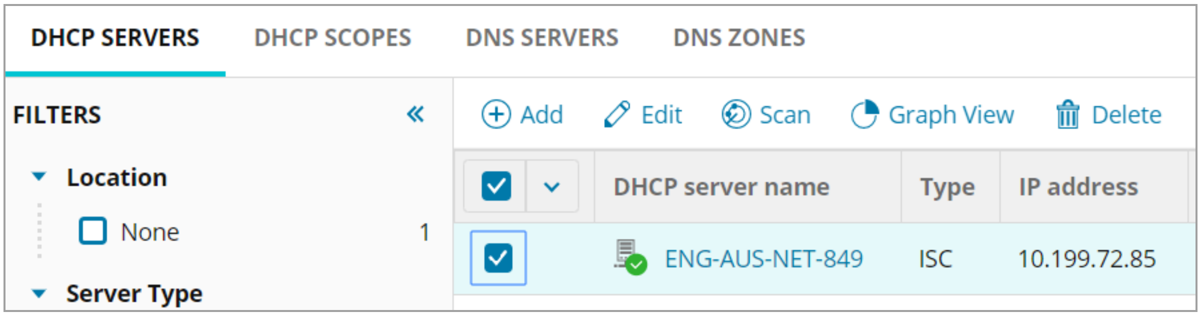
These settings will be applied upon creation. They can be changed once a subnet or scope has been added to IPAM.

☑ Enable subnet scanning to pick up additional IP Address details

Scan subnets with ICMP and SNMP every: 4 Hours

The DHCP Server is added to the DHCP & DNS Management page, and begins scanning IP address and scope lease activity.

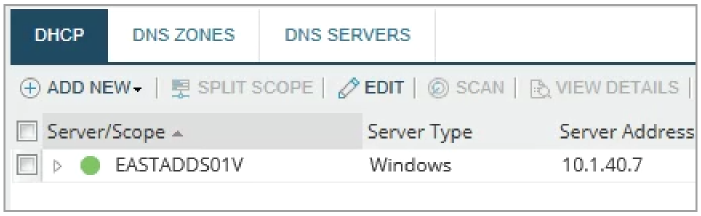
On the new DHCP & DNS Management view:



□ None 1

☑	DHCP server name	Type	IP address
☑	ENG-AUS-NET-849	ISC	10.199.72.85

On the legacy version:



□	Server/Scope	Server Type	Server Address
□	● EASTADDS01V	Windows	10.1.40.7

Edit DHCP server properties

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.
2. Click DHCP Servers (or DHCP if using the legacy dashboard) if not already selected.
3. Select the DHCP server to edit.
4. Click Edit.
5. Edit the server properties.

   ⓘ The properties available are specific to IPAM and not related to any settings on the DHCP server.

6. Click Save.

Remove a DHCP server

Remove a DHCP server from the IPAM Web Console.

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.
2. Click DHCP Servers (or DHCP if using the legacy dashboard) if not already selected.
3. Select the DHCP server to be removed.
4. Click Remove.

   A pop-up window is displayed, asking if you also want to removes scopes and corresponding subnets.

5. Click Delete Listed Items.

DHCP Impersonation

IPAM impersonates the specified account on the local computer to gain access. If the IPAM computer is not within the same windows domain as the DHCP server, the IPAM computer must have the identical account and password.

Edit a DHCP Server

The page for editing DHCP server properties can be accessed from the DHCP & DNS Management page by selecting the server and clicking Edit.

Properties

Server Type	The DHCP server type (for example, ISC or Windows). This cannot be changed.
IP Address	The IP address of this DHCP server . This cannot be changed.
Polling Engine	The polling engine / server name. This cannot be changed.
Description (optional)	A description for this DHCP server.
VLAN ID	The virtual LAN ID if applicable.
Location (optional)	The location of this DHCP.

Statistics

These fields are all display only.

Credentials

To change the credentials needed to access an existing DHCP Server, select the credential type and use an existing credential or create a new credential. See DHCP Credentials.

Custom Fields

Custom Properties can be used within IPAM the same way as with other SolarWinds products.

Other Settings

Edit Failover	Set up the failover relationships for this server. This feature is only available for Windows DHCP servers.
Server Scan Settings	Specify the frequency of scans for new scopes and leases on this server. Select whether or not to automatically add new scopes and subnets.
Scope and Subnet Settings	Select whether or not to scan subnet with ICMP and SNMP to pick up additional IP address details, and specify how often to scan.

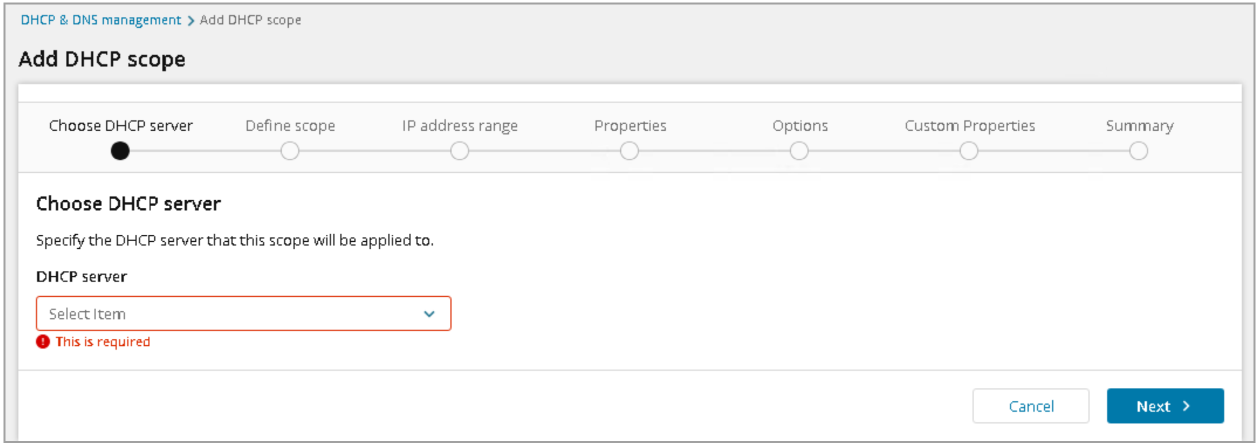
Create or edit a scope on a DHCP server

This topic includes the following sections:

A scope is a consecutive range of IP addresses that a DHCP server can draw on to fulfill an IP address request from a DHCP client. By defining one or more scopes on your DHCP server, the server can manage the distribution and assignment of IP addresses to DHCP clients.

Create a scope on a DHCP server in a non-shared network

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DHCP scope tab and click Add. The Add DHCP Scope page is displayed.



Choose DHCP server

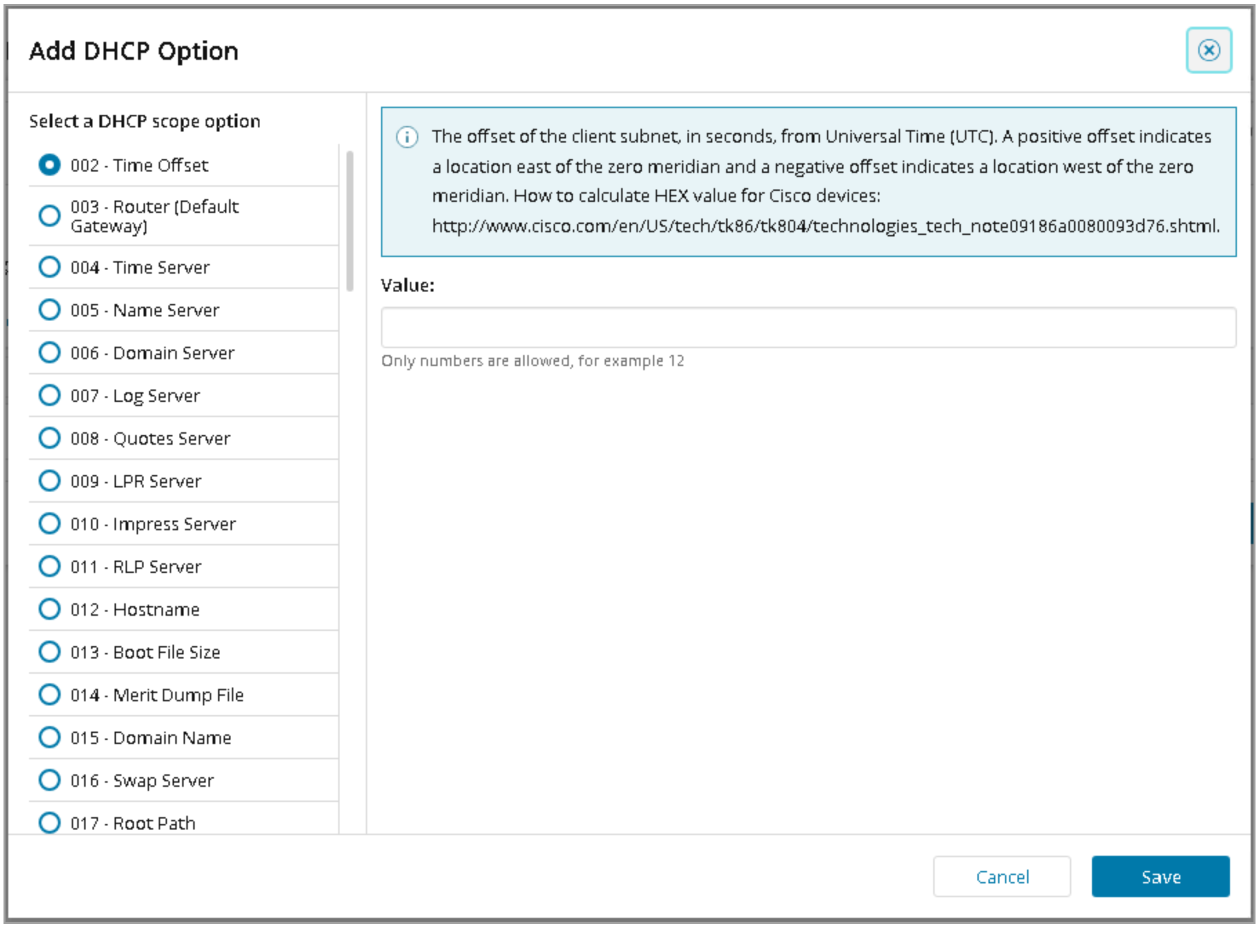
Specify the DHCP server that this scope will be applied to.

DHCP server

This is required

3. Choose the DHCP server where you want to apply the scope. Click Next.
4. On the Define Scope tab, enter the scope name, description, VLAN ID (Optional), and Location (optional). Click Next.
5. On the IP address range tab:
   a. Enter the subnet address.
   b. Click Add Exclusion to add any applicable exclusions. Enter the starting and ending ip addresses, then click Save.
   c. Adjust the CIDR if applicable.
   d. Click Next.
6. On the Options tab add any applicable scope options:

a. Click Add option to open the Add DHCP options window.



Add DHCP Option

Select a DHCP scope option

● 002 - Time Offset
○ 003 - Router (Default Gateway)
○ 004 - Time Server
○ 005 - Name Server
○ 006 - Domain Server
○ 007 - Log Server
○ 008 - Quotes Server
○ 009 - LPR Server
○ 010 - Impress Server
○ 011 - RLP Server
○ 012 - Hostname
○ 013 - Boot File Size
○ 014 - Merit Dump File
○ 015 - Domain Name
○ 016 - Swap Server
○ 017 - Root Path

The offset of the client subnet, in seconds, from Universal Time (UTC). A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. How to calculate HEX value for Cisco devices: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_tech_note09186a0080093d76.shtml.

Value:

Only numbers are allowed, for example 12

b. Select and configure the desired scope option.

c. Click save to save your scope option configuration.

d. Repeat the steps above as necessary for additional scope options.

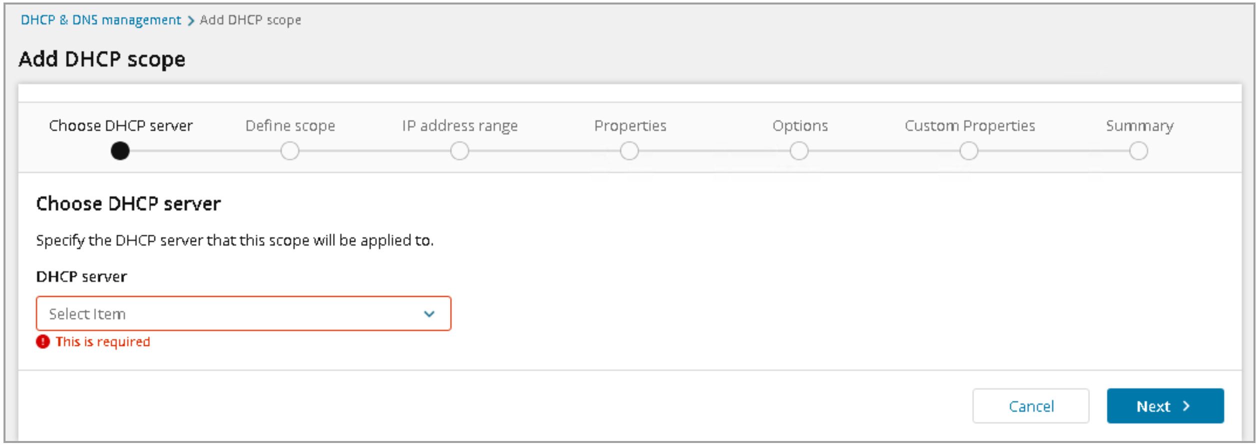
e. Click Next.

7. On the Custom Properties tab, Click Manage custom properties to open Custom Properties. Click Next. See Custom Properties for information about custom properties.

8. Review your DHCP scope settings on the Summary tab. Click Add Scope.

Create a scope on a DHCP server in a Shared Network

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DHCP scope tab and click Add. The Add DHCP Scope page is displayed.



DHCP & DNS management > Add DHCP scope

Add DHCP scope

Choose DHCP server

Specify the DHCP server that this scope will be applied to.

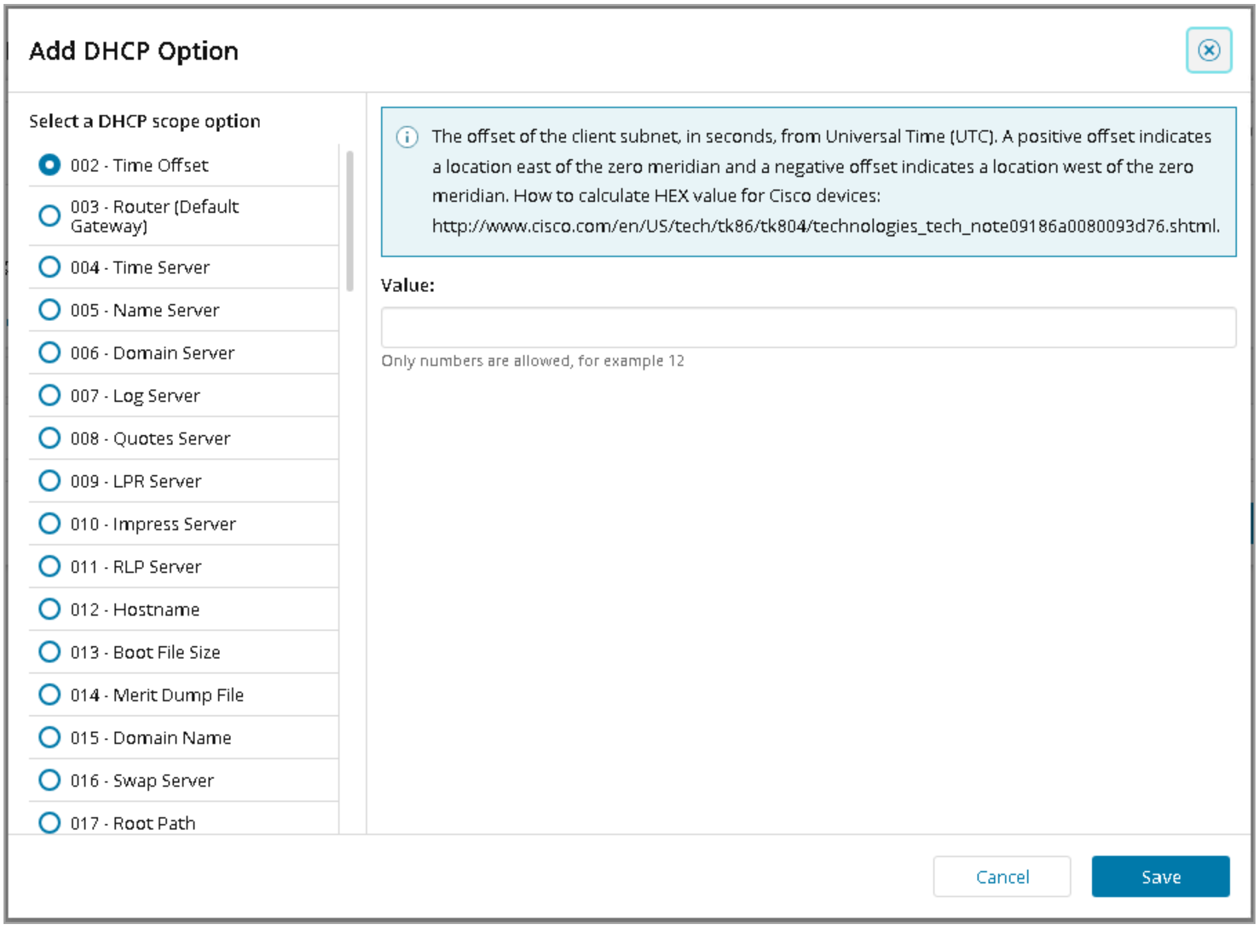
DHCP server

Select Item

This is required

3. Choose the DHCP server where you want to apply the scope. Click Next.
4. On the Define Scope tab:
   a. Select whether to use a shared network (optional).
   b. Enter the subnet address and adjust the CIDR.
   c. Select whether to automatically add discovered IP addresses to this subnet.
   d. Enter a scope description (optional), VLAN ID (optional), and Location (optional).
   e. Click Next.
5. On the IP address range tab add pools and IP address ranges you want to include:
   a. Click Add pool. Add a starting IP address and Ending Ip address. Click Save.
   b. Click Add range. Add a starting IP address and Ending Ip address. Click Save.
   c. Click Next.
6. On the Properties tab, specify a time period or set the lease time to unlimited for the Default lease time, Minimum lease time, and Maximum lease time. Click Next.
7. On the Options tab add any applicable scope options:

a. Click Add option to open the Add DHCP options window.



Add DHCP Option

Select a DHCP scope option

● 002 - Time Offset
○ 003 - Router (Default Gateway)
○ 004 - Time Server
○ 005 - Name Server
○ 006 - Domain Server
○ 007 - Log Server
○ 008 - Quotes Server
○ 009 - LPR Server
○ 010 - Impress Server
○ 011 - RLP Server
○ 012 - Hostname
○ 013 - Boot File Size
○ 014 - Merit Dump File
○ 015 - Domain Name
○ 016 - Swap Server
○ 017 - Root Path

The offset of the client subnet, in seconds, from Universal Time (UTC). A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. How to calculate HEX value for Cisco devices: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_tech_note09186a0080093d76.shtml.

Value:

Only numbers are allowed, for example 12

b. Select and configure the desired scope option.

c. Click save to save your scope option configuration.

d. Repeat the steps above as necessary for additional scope options.

e. Click Next.

8. On the Custom Properties tab, Click Manage custom properties to open Custom Properties. Click Next. See Custom Properties for information about custom properties.

9. Review your DHCP scope settings on the Summary tab. Click Add Scope.

Create a scope on a DHCP server (Legacy Wizard)

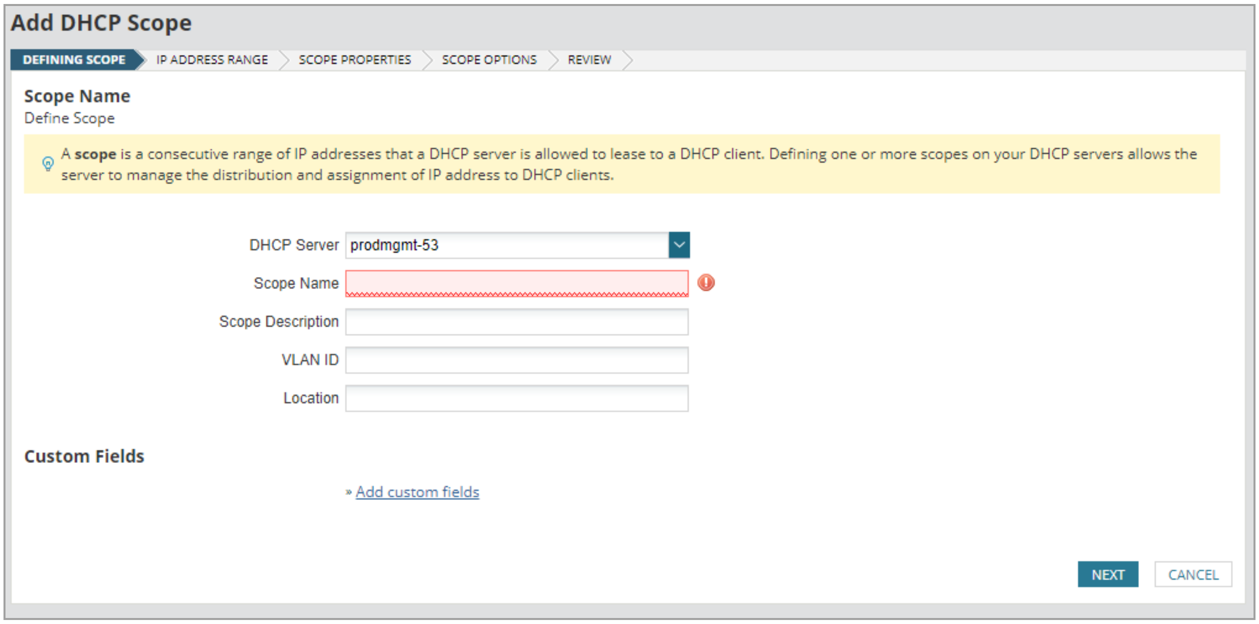
Note: The following directions apply to the Legacy DHCP scope wizard.

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.

2. Select the DHCP scope tab, and click Add.

ⓘ If you are using the legacy version of this page, select the DHCP Server tab, click Add New and select DHCP Scope.

The Add DHCP Scope page is displayed.



Add DHCP Scope

Scope Name

Define Scope

A **scope** is a consecutive range of IP addresses that a DHCP server is allowed to lease to a DHCP client. Defining one or more scopes on your DHCP servers allows the server to manage the distribution and assignment of IP address to DHCP clients.

DHCP Server: prodmgmt-53

Scope Name:

Scope Description:

VLAN ID:

Location:

Custom Fields

3. On the Defining Scope tab, enter the scope name, description, and other information, and click Next.
4. On the IP Address Range tab, enter the start and end IP addresses for the scope.
5. If you need to exclude any IP addresses from this range:
   a. Click Add Exclusion.
   b. Enter the start and end IP addresses for the exclusion range, and click Save.
6. Click Next.
7. On the Define Scope Properties tab, click Next unless you need to amend the default DHCP Offer Delay period.
8. On the Scope Option, advanced users can add or edit DHCP Scope Options. Click Next.

ⓘ For more information, see Define scope options on a DHCP server.

9. Review the settings you have entered and click Create Scope to continue.

Edit a scope on a DHCP server (Legacy Wizard)

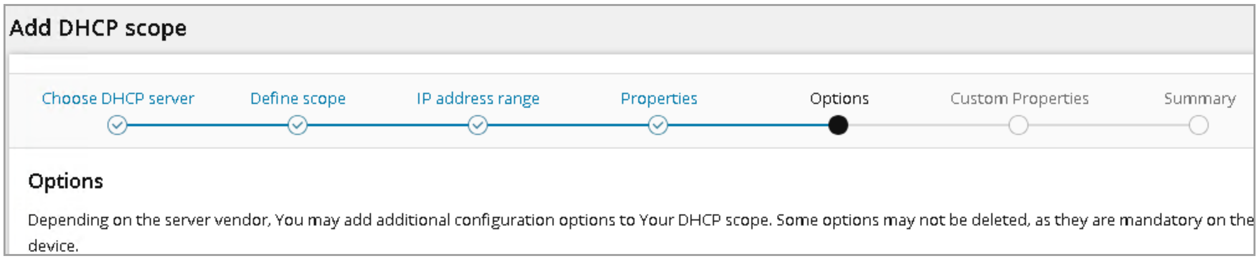
ⓘ Note: The following directions apply to the Legacy DHCP scope wizard.

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DHCP Scopes tab.

   If you are using the legacy version, select DHCP Servers, and expand the Server containing the scope.
3. Select the checkbox for the required scope and click Edit.
4. Edit the contents of each tab of the Edit DHCP page as required.
5. On the Review tab, click Update Scope.

Define scope options on a DHCP server

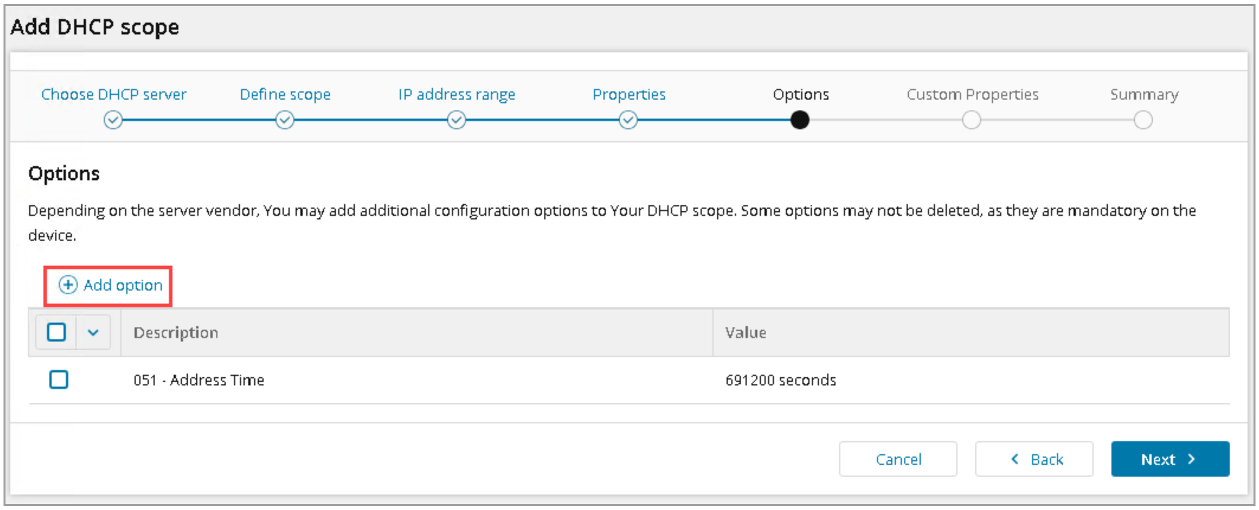
IPAM supports the majority of DHCP scope options defined within the RFC 2132 standard. The Scope Options tab is available when creating or editing a scope.


Add DHCP scope

Options

Depending on the server vendor, You may add additional configuration options to Your DHCP scope. Some options may not be deleted, as they are mandatory on the device.

The available options vary depending on the server vendor. Click **Add option** to add options.


Add DHCP scope

Options

Depending on the server vendor, You may add additional configuration options to Your DHCP scope. Some options may not be deleted, as they are mandatory on the device.

□	Description	Value
□	051 - Address Time	691200 seconds

Set up VoIP options (66 and 67) on your scopes.

Unsupported DHCP options

The following options are unsupported:

Unsupported Windows DHCP Server options

- 39 TCP Keepalive Data
- 58 Renewal Time Value
- 59 Rebinding Time Value
- There is no UI option to create option 58 and 59 on a Windows DHCP server. They are simply a function of lease time (option 51).

Unsupported Cisco DHCP Server options

- 12 Host Name
- 50 Address Request
- 52 Overload
- 53 DHCP Msg Type
- 54 DHCP Server Id
- 58 Renewal Time
- 59 Rebinding Time
- 61 Client Id

Unsupported ISC DHCP server options

- 50 Address Request
- 53 DHCP Message Type
- 54 DHCP Server Identifier
- 56 DHCP Message
- 58 Renewal Time
- 59 Rebinding Time

Configure split scopes on DHCP servers

You may want to split a DHCP scope in order to provide load balancing between two DHCP servers and ensure high availability DHCP services for your network.

> ⓘ
> - You must have two DHCP servers of the same type to be able to split a scope between them
> - Splitting scopes on some Cisco DHCP servers may require that you perform additional configuration steps on the servers themselves. See your Cisco documentation for more information.

Scopes are usually split into one of two configurations:

- 50/50: half of the IP addresses are on the primary DHCP server and half are on the secondary server. This configuration is usually used for load balancing.
- 80/20: 80% of the IP addresses are on the primary DHCP server and 20% are on the secondary server. This configuration is generally used to ensure high availability.

When a scope is split, the result is two scopes, each of which excludes the IP addresses the other scope (and server) manages.

When you split a scope, you can specify a delay for the secondary scope. If you are using a secondary scope to ensure high availability, this should be set to 1000 - 5000ms to ensures the primary server has time to respond to DHCP requests, so that the secondary scope is only used if there are problems. For load balancing however, this should be set to zero so that both scopes can respond to requests immediately.

For example, scope01 is on your primary DHCP server. Scope01 includes the entire subnet of 10.10.10.0/24 (254 IP addresses), with no exclusions. You split scope01, and name the second scope scope02 on your secondary DHCP server. You choose an 80/20 split.

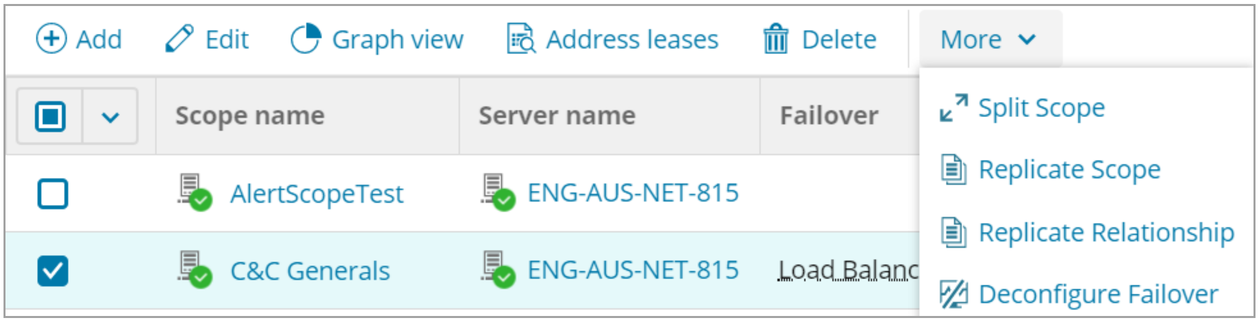
Scope01 still spans the entire subnet, but excludes the last 20% of the addresses in that subnet (10.10.10.204-254). Scope02 also spans the entire subnet, but excludes the first 80% of the addresses in that subnet (10.10.10.1-203).

To split a scope:

1. Go to My Dashboards > DHCP & DNS Management.
2. Select the DHCP Scope tab.

   ⓘ If using the legacy version of this view, select the DHCP Server and expand the server with the required scope.

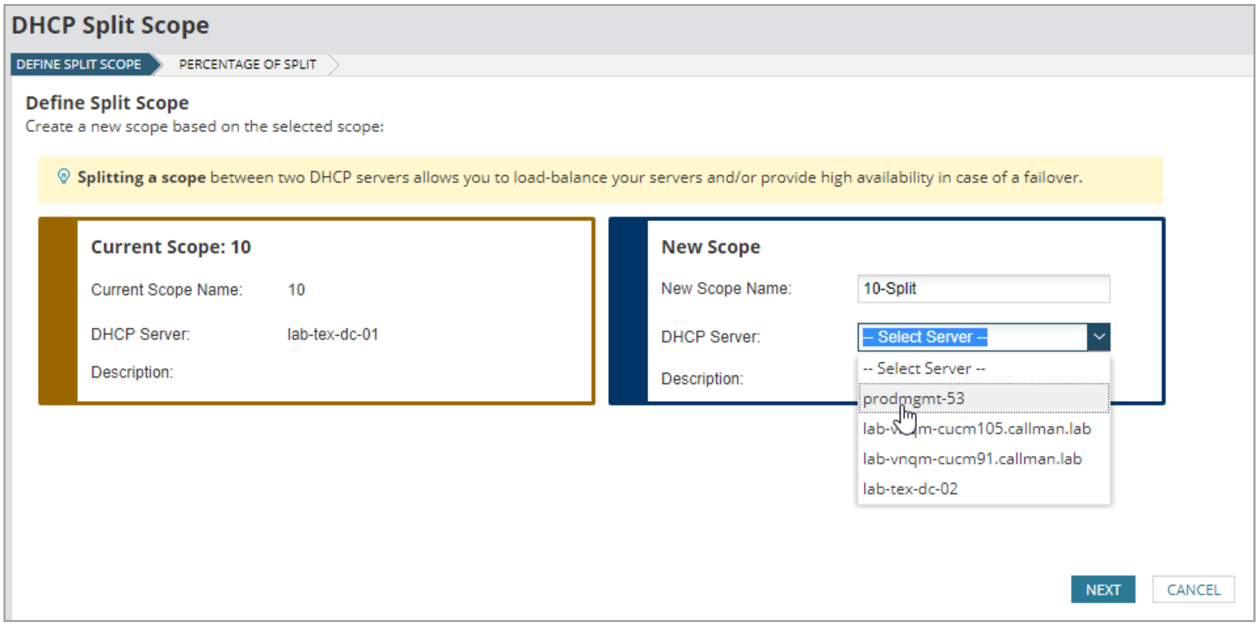
3. Select the scope to be split.
4. Click More, then select Split Scope from the menu.



	Scope name	Server name	Failover
□	AlertScopeTest	ENG-AUS-NET-815	
☑	C&C Generals	ENG-AUS-NET-815	Load Balanc

   ⓘ If using the legacy view, select Split Scope from the Scopes menu.

The Define Split Scope page is displayed.



DHCP Split Scope

Define Split Scope

Create a new scope based on the selected scope:

Splitting a scope between two DHCP servers allows you to load-balance your servers and/or provide high availability in case of a failover.

Current Scope: 10

Current Scope Name: 10

DHCP Server: lab-tex-dc-01

Description:

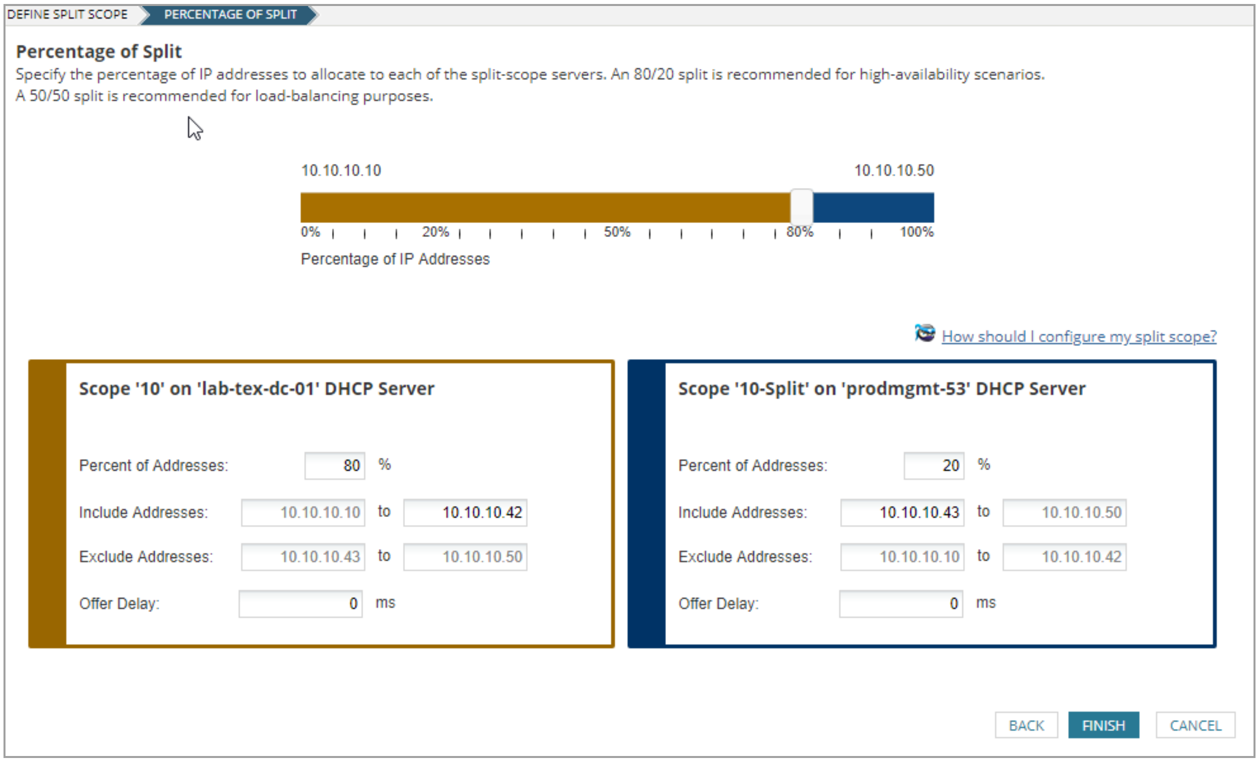
New Scope

New Scope Name: 10-Split

DHCP Server: -- Select Server --

Description:

5. Enter a name for the secondary scope, select the server, and click Next.



Percentage of Split

Specify the percentage of IP addresses to allocate to each of the split-scope servers. An 80/20 split is recommended for high-availability scenarios. A 50/50 split is recommended for load-balancing purposes.

10.10.10.10
10.10.10.50
0%
20%
50%
80%
100%
Percentage of IP Addresses
How should I configure my split scope?

Scope '10' on 'lab-tex-dc-01' DHCP Server

Percent of Addresses: 80 %

Include Addresses: 10.10.10.10 to 10.10.10.42

Exclude Addresses: 10.10.10.43 to 10.10.10.50

Offer Delay: 0 ms

Scope '10-Split' on 'prodmgmt-53' DHCP Server

Percent of Addresses: 20 %

Include Addresses: 10.10.10.43 to 10.10.10.50

Exclude Addresses: 10.10.10.10 to 10.10.10.42

Offer Delay: 0 ms

6. Drag the slider to specify the split required. The default is 80%, as recommended for high-availability scenarios. Set to 50% for load balancing.

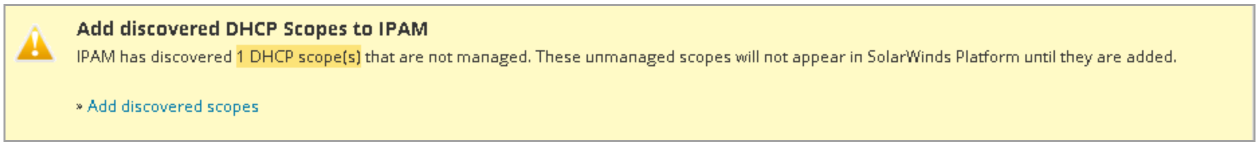
7. Set the Offer Delay for the secondary scope.

   > This should be 1000-5000ms for high availability scenarios, zero for load balancing.

8. Click Finish.

Discovered Scopes

If IPAM finds unmanaged scopes on your network, a message will be displayed on both the DHCP & DNS Management and IPAM Settings pages.

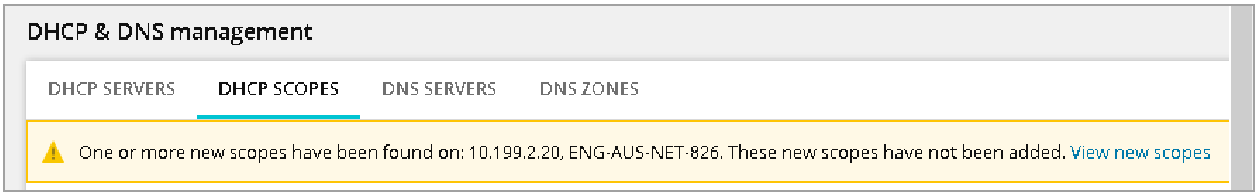


Add discovered DHCP Scopes to IPAM

IPAM has discovered 1 DHCP scope(s) that are not managed. These unmanaged scopes will not appear in SolarWinds Platform until they are added.

» Add discovered scopes

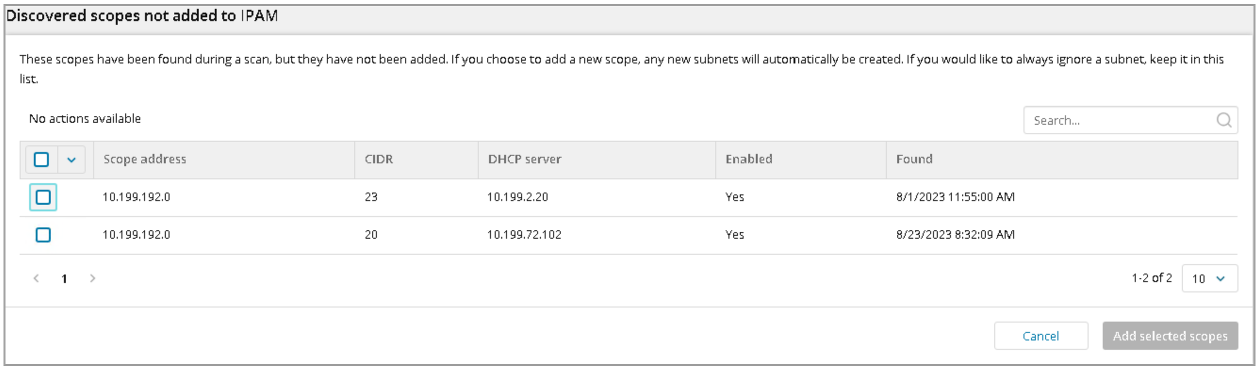
Click Add discovered scopes to display the Discovered Scopes, Not Added to IPAM page.



DHCP & DNS management

One or more new scopes have been found on: 10.199.2.20, ENG-AUS-NET-826. These new scopes have not been added. View new scopes

Click View new scopes to display the Discovered Scopes, Not Added to IPAM page.



Discovered scopes not added to IPAM

These scopes have been found during a scan, but they have not been added. If you choose to add a new scope, any new subnets will automatically be created. If you would like to always ignore a subnet, keep it in this list.

No actions available

□	Scope address	CIDR	DHCP server	Enabled	Found
□	10.199.192.0	23	10.199.2.20	Yes	8/1/2023 11:55:00 AM
□	10.199.192.0	20	10.199.72.102	Yes	8/23/2023 8:32:09 AM

Here you can add the discovered scopes to IPAM, or ignore.

Remove a scope

1. Go to My Dashboards > My Dashboards > DHCP & DNS Management.
2. Click the DHCP Scopes tab, select the DHCP scope to be removed, and click Delete.

   ⓘ If using the legacy version of this view, select the DHCP Server tab, expand the server on which the scope is located, and click Remove.

   Information specific to the scope to be removed is displayed.
3. Select whether you want to remove the scope from the server.

   ⚠ Further information is displayed if removing the scope from the server will be harmful.
4. Click Delete.

Address Leases for...

Go to My Dashboards > DHCP & DNS management, and click DHCP Scopes. Select a scope and click Address Leases to display the Address Leases window.

If address leases are found for the selected DHCP scope, the following information is displayed.

Client IP Address	The IP address leased to the client.
Client Name	The name of the client to whom this IP Address is leased.
Lease Expiration	The lease expiry time and date.
Type	Dynamic or Static.
Client Status	The status of this lease, which can be reserved or used. If used, there will a lease expiry time and date.
Unique ID	The unique 12-character identifier for this lease.

Set up and monitor Windows DHCP server failover

With IPAM you can configure failover across multiple scopes using a single screen, whereas in Windows Server you can only configure failover one scope at a time.

IP Address Manager fully supports the DHCP failover feature set implemented in Windows Server 2012 and later versions.

- For further information about DHCP failover options in Windows Server 2012 and later, see the Microsoft TechNet guide, Understand and Deploy DHCP Failover (© 2016 Microsoft, available at https://microsoft.com, obtained on November 26, 2018).
- Failover is not supported for Cisco, ISC or Infoblox DHCP environments.

View DHCP failover details in IPAM

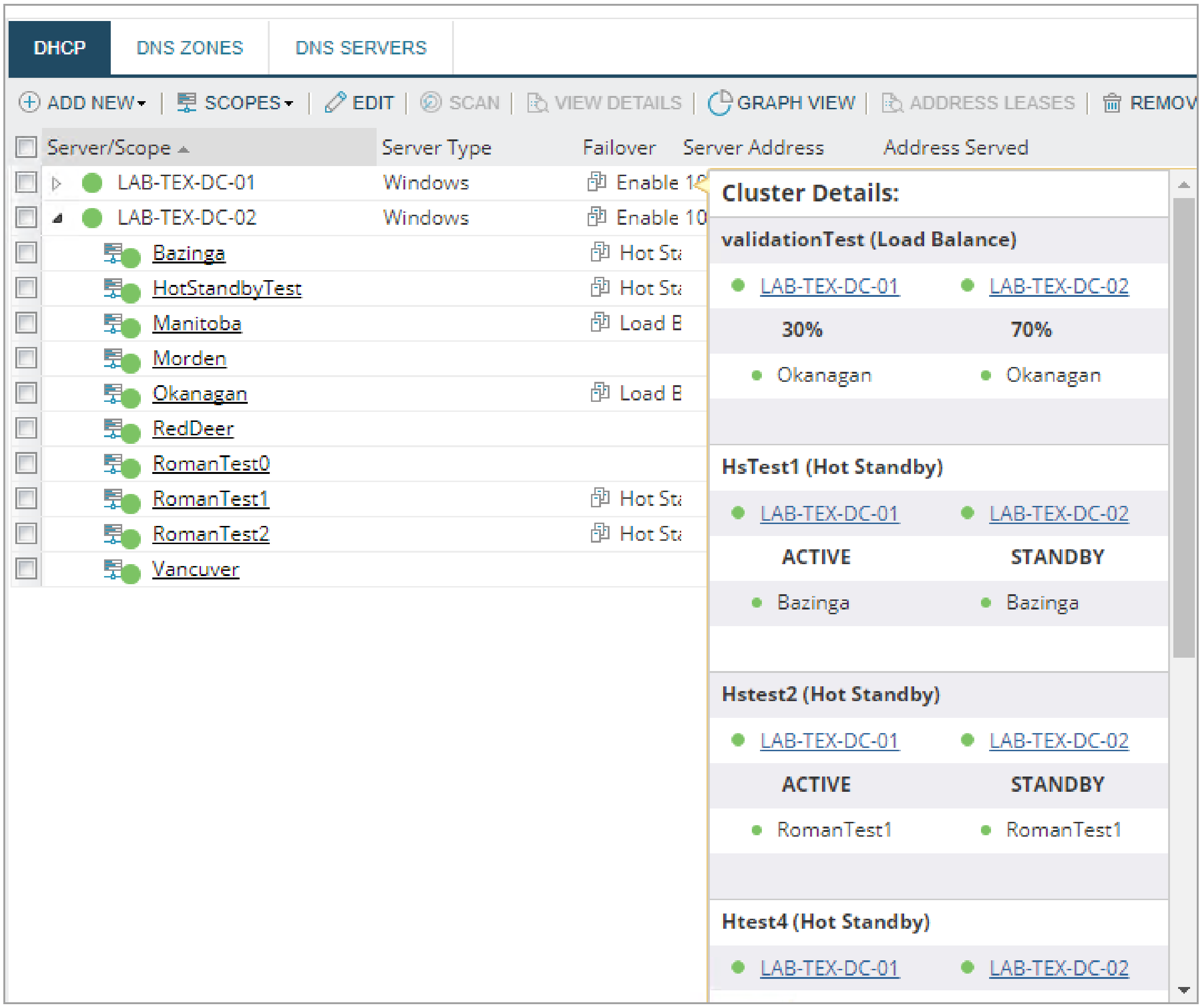
1. Open the SolarWinds Web Console and navigate to My Dashboards > IP Addresses > DHCP & DNS Management.

   Select the DHCP Server tab.

   If using the legacy view, select the DHCP tab.

2. Select the required server, and move the cursor over the Failover column for the required Server.

   IPAM consolidates cluster details into a single pop-up, whereas Windows Server only displays failover details one scope at a time.



□	Server/Scope	Server Type	Failover	Server Address	Address Served
□	LAB-TEX-DC-01	Windows	Enable 1		
□	LAB-TEX-DC-02	Windows	Enable 10		
□	Bazinga		Hot St		
□	HotStandbyTest		Hot St		
□	Manitoba		Load B		
□	Morden				
□	Okanagan		Load B		
□	RedDeer				
□	RomanTest0				
□	RomanTest1		Hot St		
□	RomanTest2		Hot St		
□	Vancuver				

Cluster Details:

validationTest (Load Balance)	
● LAB-TEX-DC-01	● LAB-TEX-DC-02
30%	70%
● Okanagan	● Okanagan

HsTest1 (Hot Standby)	
● LAB-TEX-DC-01	● LAB-TEX-DC-02
ACTIVE	STANDBY
● Bazinga	● Bazinga

Hstest2 (Hot Standby)	
● LAB-TEX-DC-01	● LAB-TEX-DC-02
ACTIVE	STANDBY
● RomanTest1	● RomanTest1

Htest4 (Hot Standby)	
● LAB-TEX-DC-01	● LAB-TEX-DC-02

Create or Edit DHCP failover details in IPAM

1. Open the SolarWinds Web Console and choose My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DHCP Server tab.

   ⓘ If using the legacy view, select the DHCP tab.

3. Select the required server, and click Edit.

   The Edit <Server> Properties dialog box opens.

4. Scroll down to the Edit Failover section, and edit the required information.

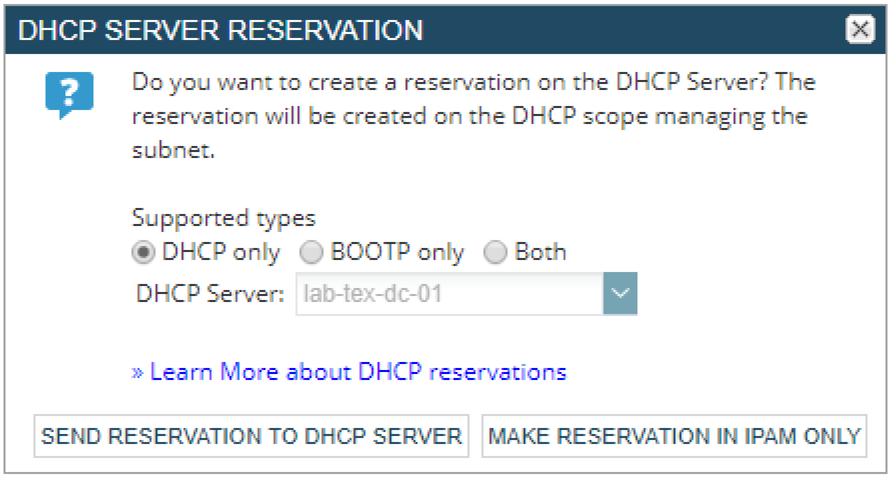
   ⓘ To configure DHCP failover from IPAM, both DHCP servers must be managed by IPAM.

5. Click Save to save your changes.

Reserve an IP Address on a Windows DHCP server

The following steps update the reservation status of an IP address on a Windows DHCP server:

1. Go to My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Navigate to the subnet containing in the IP Address View.
3. Select the IP address and click Set Status.
4. Set the status to Reserved.
5. Select the type of reservation and the DHCP Server to use, if applicable.



DHCP SERVER RESERVATION

Do you want to create a reservation on the DHCP Server? The reservation will be created on the DHCP scope managing the subnet.

Supported types

● DHCP only ○ BOOTP only ○ Both

DHCP Server: lab-tex-dc-01

» Learn More about DHCP reservations

SEND RESERVATION TO DHCP SERVER
MAKE RESERVATION IN IPAM ONLY

- Click Send Reservation to DHCP Server, if you want to make an actual reservation on the DHCP scope managing this subnet.
- Click Make Reservation in IPAM Only, if you only want to make the reservation in the IPAM database.

Troubleshooting DHCP and DNS connections in IPAM

Problem	Description	Resolution
Bad username or password	This error may occur when the valid user account on the SolarWinds host has no meaning to the DHCP Server or when the provided password is not correct on the DHCP Server.	• Verify the account used is valid on the DHCP Server. • Verify that the provided account and password is both identical and functional on both the SolarWinds host and DHCP Server.

Problem	Description	Resolution
The RPC Server is Unavailable	This error may occur when the DHCP Server is unable to receive or respond to RPC Requests.	• Verify that there is no firewall preventing the SolarWinds host from performing RPC calls by checking with Administrator accounts that Windows file sharing is possible. An alternate way to verify is a telnet to the IP address provided in the SolarWinds node on port 445. • If this occurs intermittently, verify that the DHCP server has enough client access licenses.
Insufficient permissions	Insufficient permissions	• Verify that the provided user account is part of the DHCP Users group in the DHCP Server. • For Cisco DHCP, verify the requirements on Cisco DHCP device for SolarWinds IPAM.
BIND Credential fails using ssh or telnet option	When adding a DNS Bind, in the BIND Credential option there is a space in the Credential name. For example: Credential Name: `Bind 1` Username: `root` Password: `1234`	Remove the space in the 'Credential Name' (should be Bind1)
BIND DNS on AIX Symptom: Bind is not running error when testing the connection to implement BIND DNS Mgmt and add an AIX 6.1 Bind9 based DNS Server	When the named-V and ps -A -o comm,pid,args | grep ^named commands are issued and parsing returns a value that does not match the criteria, the application is not enabled: named9 vs named	Perform a manual configuration of the config file by renaming the file from named9 to named.

IPAM BIND Requirements

- User account needs to be configured to allow remote telnet or SSH access to BIND machine.
- Read and write file access is required for all BIND configuration files.
    - `/etc/named.conf`, and all included files
    - all zone data files
- Read and write access to system temp directory /tmp
- IPAM utilizes both standard Linux commands (POSIX) and BIND specific commands that are required for IPAM BIND management functionality:

```
named
ps
grep
sha1sum
cat
if [ -r "filepath" ] ; then echo 'true'; else echo 'false'; fi
if [ -w "filepath" ] ; then echo 'true'; else echo 'false'; fi
if [ $? -eq 0 ] ; then echo 'true'; else echo 'false'; fi
cp
mkdir
rm
named-checkconf
```

ARP table

The ARP table is where the responses to previous ARP requests are cached. IPAM utilizes a feature called Neighbor Scanning as an additional method of retrieving information. Neighbor Scanning pulls information from the ARP table of neighboring devices when ICMP and SNMP is blocked or disabled.

IPAM first checks if the device is capable of SNMP and supports ARP table:

To check whether SNMP is available, use the following OID:

- OidSysContact "1.3.6.1.2.1.1.4.0" iso.org.dod.internet.mgmt.mib-2.system.sysContact.0

To check whether the ARP table is available, use the following OID:

- OidIPNetToMediaTable "1.3.6.1.2.1.4.22" iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTable

The IPNetToMediaTable is pulled for client information. If the device supports this table, then IPAM can work with it.

Monitor and Manage DNS servers in IPAM

The following section covers how IPAM can monitor and manage your DNS servers.

ⓘ Since Infoblox monitoring is read-only certain DNS operations are unavailable. For further information see Monitor the Infoblox environment.

ISC DNS server settings in IPAM

The following settings and specifications are required for IPAM to access your ISC DNS servers.

ⓘ Nested configurations are **not** supported.

Base version for ISC	BIND9.1+
Operating system	POSIX compliant Linux distributions

User access	• User account configured to enable remote telnet* or SSH access to ISC DS machine * The root account cannot be used in telnet. Also, a banner is required in telnet in the form: " <empty line> Some customer telnet message " • Read and write file access for users on the configuration files
CLI commands	• dhcpd --version • named -V • named-checkconf -z "$FILE_PATH" • uname -mrs • ps -A -o comm,pid,args \| grep ^named • if [-r '$FILE_PATH'] ; then echo 'true'; else echo 'false'; fi • if [-w '$FILE_PATH'] ; then echo 'true'; else echo 'false'; fi • sha1sum • cat • mkdir -p "/tmp/SolarWinds/IPAM/var/cache/bind" • rm -r -f "/tmp/SolarWinds/IPAM" • cp -f -p --parents /etc/$FILE_PATH /tmp/SolarWinds/$FILE_PATH • cp -r -u -f -b -S.backup -p "/tmp/SolarWinds/IPAM/$FILE_PATH" "/var/cache/$FILE_PATH" • rndc reload • kill -s SIGHUP $PID
Configuration file	IPAM seeks the configuration file in one of the following path: • /etc/named.conf If the default file path is different for your distribution you may of course create a soft link. Or create /etc/named.conf file, and include rest of configuration files in it.

Lease file	• `"/var/db/dhcpd.leases”` • `"/var/lib/dhcpd/dhcpd.leases"` • `"/var/lib/dhcp/dhcpd.leases"` • `"/var/db/dhcpd/dhcpd.leases"`

Configure an ISC DNS server

On a new installation of ISC DHCP from a terminal prompt:

1. Enter the following command to install the DNS server program:

   ```
   apt-get install bind9 bind9utils
   ```

   or:

   ```
   apt install bind9 bind9utils
   ```

   (depending on the Debian/Ubuntu version)

   For Centos/RHEL, enter:

   ```
   yum install bind
   ```

2. To change the default configuration, edit the file:

   ```
   /etc/named.conf
   ```

3. Assign a static IP to the interface that you use for DHCP.

   ⓘ Verify that the ISC service is running so IPAM can communicate with your ISC DNS server. After you edit the configuration file, restart the service.

To begin managing your ISC servers, they must first be added to IPAM. See Add DNS servers to IPAM for more information.

Add a DNS server

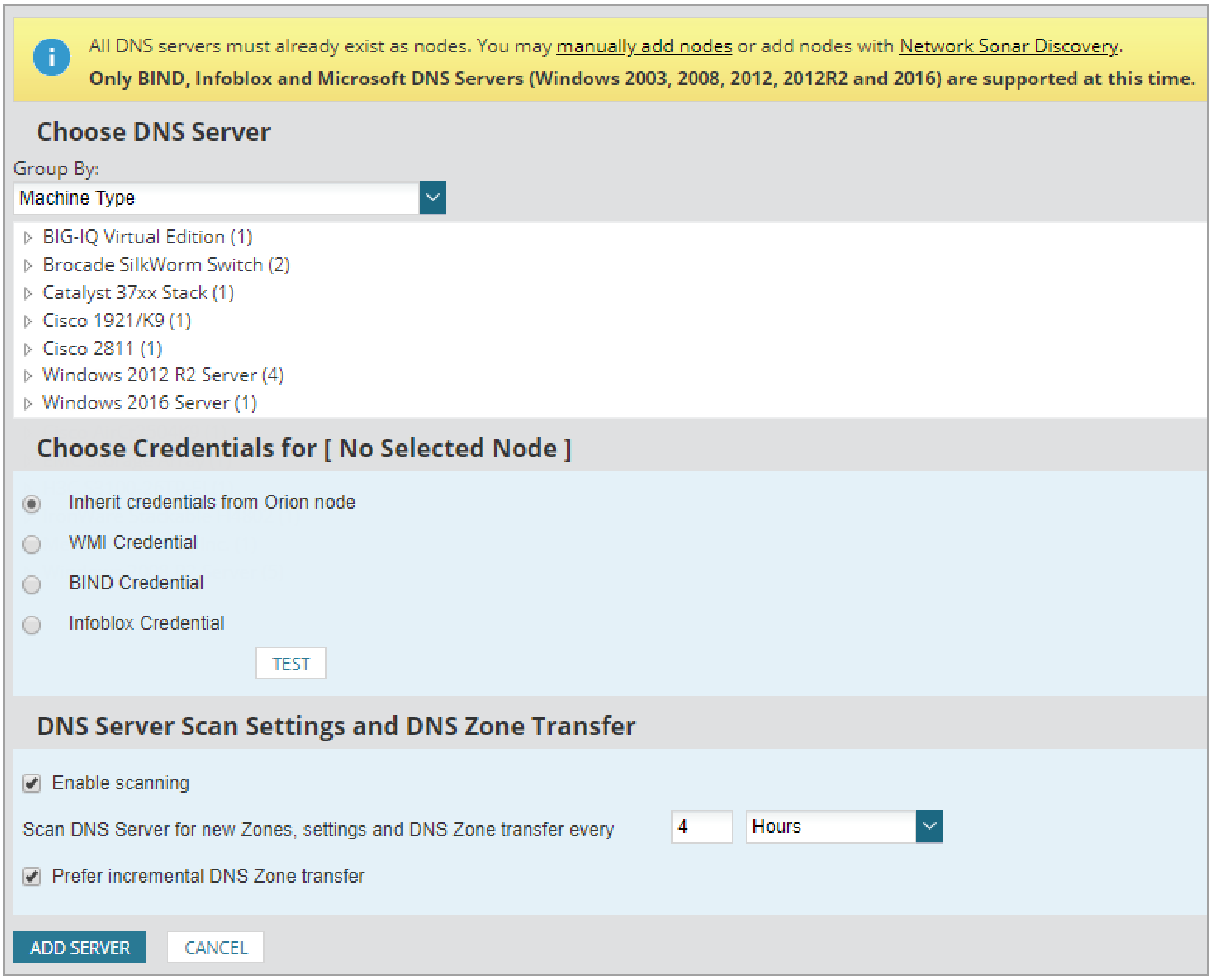
All DNS servers must already exist as nodes in your installation before they can be added to IPAM.

> ⓘ Windows DNS Servers 2003, 2008, 2012, 2012R2, 2016 2019, and 2022 are supported.
>
> Bind DNS 9.1 through 9.11.*n* are supported.
>
> Some environments may require you to grant read-only access to a non-administrator account. See Grant read-only access to non-administrator accounts for IPAM DNS Monitoring for more information.

1. Go to My Dashboard > DHCP & DNS Management.
2. Click on the DNS Server tab to display the current list of DNS servers.
3. Click Add.

> ⓘ If using the legacy view, click Add New > DNS Server.

4. Select a DNS Server from the list. If the server is not shown, use the Group By menu to sort the DNS servers listed to aid identification.



All DNS servers must already exist as nodes. You may manually add nodes or add nodes with Network Sonar Discovery.
Only BIND, Infoblox and Microsoft DNS Servers (Windows 2003, 2008, 2012, 2012R2 and 2016) are supported at this time.

Choose DNS Server

Group By: Machine Type

- BIG-IQ Virtual Edition (1)
- Brocade SilkWorm Switch (2)
- Catalyst 37xx Stack (1)
- Cisco 1921/K9 (1)
- Cisco 2811 (1)
- Windows 2012 R2 Server (4)
- Windows 2016 Server (1)

Choose Credentials for [No Selected Node]

● Inherit credentials from Orion node
○ WMI Credential
○ BIND Credential
○ Infoblox Credential

DNS Server Scan Settings and DNS Zone Transfer

☑ Enable scanning
Scan DNS Server for new Zones, settings and DNS Zone transfer every 4 Hours
☑ Prefer incremental DNS Zone transfer

5. Enter or select the credentials for this server. WMI credentials can be inherited from the node to the DNS server.

6. Click Test to confirm.

   ⓘ If you provide Windows credentials for accessing and receiving information through WMI, you must provide the account name in the following order: Domain or Computer Name\User Name for domain level authentication or user name for workgroup level authentication.

7. Select Enable Scanning to enable incremental DNS Zone transfers. IPAM scans the DNS server for new zones and settings based upon the interval time.
8. Click Add Server. The DNS Zones are displayed.

DNS server WMI permissions

The following section details the permissions required for IPAM users to monitor DNS servers.

Enable an account for WMI

A DNS server administrator account that can make changes on the DNS server is required to manage DNS servers. If you have a stand-alone DNS server, you can use a local administrator account configured for WMI access.

ⓘ Administrator accounts are configured to make DNS server management tasks by default. For an AD and DNS setup, this is an account with full DACL (discretionary access control list) with remote WMI management enabled

Grant read-only access to non-administrator accounts for IPAM DNS monitoring

To poll the DNS server without an administrator account, you must add the user to the DNS Admin group. The account must have Read/Write permissions for DNS management so the account is able to write itself to the DNS server as a zone transfer server. Administrators can specify the rights of a user within their account settings to have just read only access to the DNS portion of IPAM.

Enable an account for WMI

Use the DNS Server Administrator account based on your network configuration.

- In Standalone DNS, administrators are configured to make DNS server management tasks by default.

- In a AD+DNS setup, use the account with full DACL to manage the DNS Server. The account must have remote WMI for management enabled.

The following steps detail how to use a non-administrator account.

To configure DCOM services

1. Start `dcomcnfg`.
2. Expand Component Services\Computers, right-click My Computer, and select Properties.
3. Click the COM Security tab.
4. In the Access Permissions group:
   - Click Edit Default, add your account, and select Enable Local Access and Remote Access.
   - Click Edit Limits, add your account, and select Enable Local and Remote Access.
5. In the Launch and Activation permissions:
   - Click Edit Default, add your account, and select Allow all.
   - Click Edit Limits, add your account, and select Allow all.

To configure access to the WMI branch

1. Start the MMC console and add the WMI Control Snap-in.
2. Right-click Snap-in and click Properties.
3. In the Security tab, select MicrosoftDNS and CIMV2 branch, and then click Security.
4. Add your account, and Allow Execute Methods, Enable Account, Remote Enable.
5. On the DNS Security tab, verify that the new user you created has DNSAdmin rights.
6. Start `dnsmgmt.msc`.
7. Right-click the server or service and view properties to confirm that all the options for the user are selected.

To test the connection to a DNS server with specific credentials, use the Windows Management Instrumentation Tester, `wbemtest,` and connect to a machine using namespace, such as: `\\remote_hostname\root\MicrosoftDNS`

BIND permissions

IPAM offers support for Linux-based BIND DNS server monitoring and management.

The following are the minimum requirements needed to monitor BIND DNS.

- IPAM supports Debian 8.6 and 9.5, and RHEL/CentOS version 6 and 7.
- IPAM supports BIND versions BIND 9.9+, BIND 9.10+, and BIND 9.11+.

> ⓘ SolarWinds recommends using BIND 9.11+, as it supports commands for checking configuration syntax, which IPAM is able to use for configuration change validation during management operations.

Required permissions

The user account needs to be configured to enable remote telnet or SSH access to the BIND machine.

Read and write file access is required for:

- the `/etc/named.conf` directory and all included files
- the system temp directory `/tmp` for all zone data files
- the `/var/named` directory

> ⓘ The DNS zone configuration files are stored here by default - without this permission it is impossible to create/modify them.
>
> By default IPAM preserves mode, ownership and timestamps during file copying (IPAM works on copies so that it will not break anything during error) and if the user (in IPAM credentials) is not an owner of the configuration files (e.g. `/var/named`) then an `Operation not permitted` error will occur as preserving timestamps is only allowed for the target file owner (Unix/Linux mechanics).
>
> There are two options:
>
> 1. Administrator can disable timestamps preservation in the IPAM system settings by checking the “No preserve timestamps” checkbox:
>   - No additional configuration on the OS side is required – timestamps will not be preserved
> 2. OS Administrator can change the owner of the configuration files to the desired user:
>   - Not always possible (which is why the first option was implemented)
>   - This requires additional OS configuration

CLI Commands

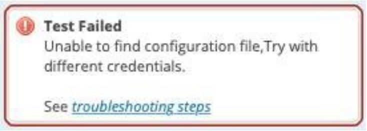
IPAM uses both standard Linux commands (POSIX) and BIND specific commands. The following are the commands used by IPAM for both management and monitoring:

- `named`
- `ps`
- `grep`
- `sha1sum`
- `cat`
- `if [ -r "filepath" ] ; then echo 'true'; else echo 'false'; fi`
- `if [ -w "filepath" ] ; then echo 'true'; else echo 'false'; fi`
- `if [ $? -eq 0 ] ; then echo 'true'; else echo 'false'; fi`
- `cp`
- `mkdir`
- `rm`
- `named-checkconf`

After you add a BIND in IPAM, your device syncs and imports BIND DNS configurations which can then be monitored or managed.

Troubleshooting

If you are unable to add a DNS server set up using the BIND 9 package for Debian distribution, and testing the credentials results in the following error:



Test Failed
Unable to find configuration file,Try with different credentials.

See *troubleshooting steps*

then please apply the following steps:

1. Log in on your DNS server machine.
2. Open the `/etc/default/bind9` file
3. Edit the OPTIONS variable by adding the configuration file path flag:

   ```
   OPTIONS="-u bind -c <path to named.conf>
   ```

   ⓘ By default `<path to named.conf>` on Debian BIND 9 is `/etc/bind/named.conf`

4. Save this change and restart the Bind9 daemon.

You should now be able to add the DNS server to IPAM without any issues.

ⓘ The reason for specifying the -c flag, even if you have the default configuration, lies in the Bind9 Debian package configuration (specified during build time). One of the commands that IPAM executes to get information about the environment is "named -V". Normally it outputs a lot of information including a sysconfdir flag pointing to the directory containing the named.conf file. Unfortunately, in the Bind9 package, the sysdirconf flag occurs twice (also pointing to `/etc & /etc/bind`) which is ambiguous to the IPAM results parser and causes it to output the "Test Failed: Unable to find configuration file" error.

IPAM DNS records

IPAM supports five DNS record types.

A	Address Mapping/Host	An A record provides the IP address of a domain. Examples: www, mail, ftp, webmail, www2, secure, store, dev
AAAA	IP Version 6 Address	Returns a 128-bit IPv6 address, most commonly used to map host names to an IP address of the host.
CNAME	Canonical Name/Alias	CNAME records map aliases with domain names. Example: Record: webmail Address: mail.hostedmail.com
MX	Mail exchanger	MX records use your external mail servers to process your email. Example: Priority: 10 Record: @ Address: mail.domain.com
PTR	Reverse-lookup Pointer	A domain name pointer maps a network interface (IP) to a host name.

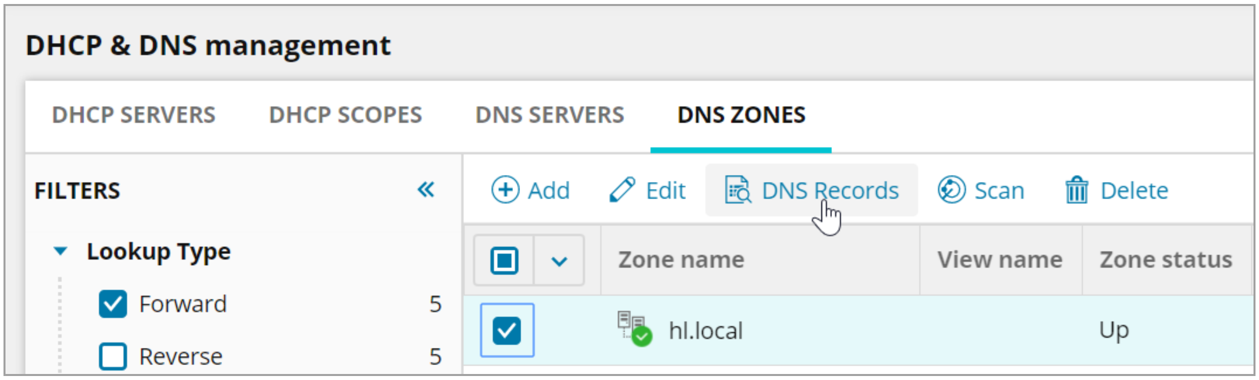
Currently you cannot edit HINFO, ISDN, NS or SOA records.

Each DNS record can be customized as needed.

- IPAM automatically detects DNS forward and reverse mismatches.
- IPAM automatically creates DNS PTR records when new devices are added into DNS zones.
- From this location you can manage all aspects of your domain registration. You can also change your domain name servers.

View DNS records

1. Go to My Dashboard > DHCP & DNS Management.
2. Click on the DNS Zone tab and select a zone name.
3. Click DNS Records.

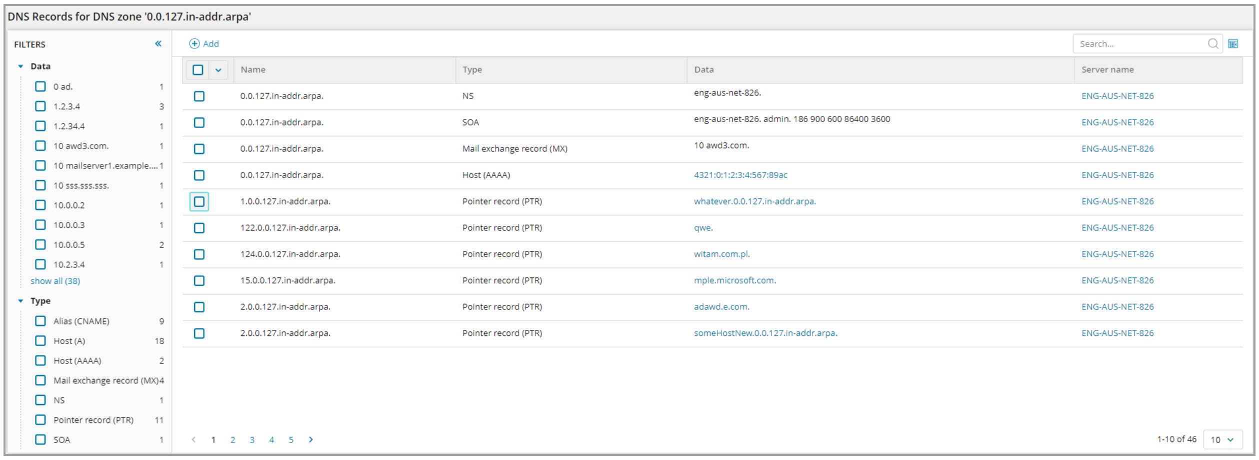


Lookup Type

- ☑ Forward 5
- □ Reverse 5

☐	Zone name	View name	Zone status
☑	hl.local		Up

The DNS Records for this zone is displayed.


DNS Records for DNS zone '0.0.127.in-addr.arpa'

Data

□ 0 ad.	1
□ 1.2.3.4	3
□ 1.2.34.4	1
□ 10 awd3.com.	1
□ 10 mailserver1.example....	1
□ 10 sss.sss.sss.	1
□ 10.0.0.2	1
□ 10.0.0.3	1
□ 10.0.0.5	2
□ 10.2.3.4	1

show all (38)

Type

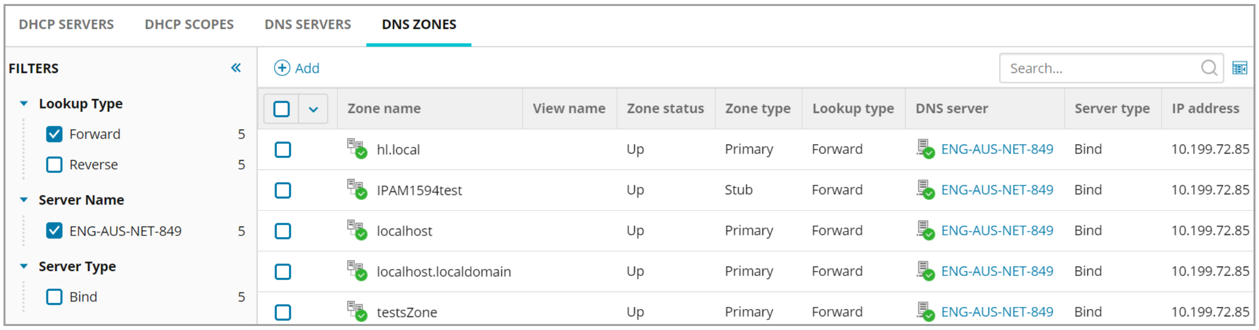
□ Alias (CNAME)	9
□ Host (A)	18
□ Host (AAAA)	2
□ Mail exchange record (MX)	4
□ NS	1
□ Pointer record (PTR)	11
□ SOA	1

□	Name	Type	Data	Server name
□	0.0.127.in-addr.arpa.	NS	eng-aus-net-826.	ENG-AUS-NET-826
□	0.0.127.in-addr.arpa.	SOA	eng-aus-net-826. admin. 186 900 600 86400 3600	ENG-AUS-NET-826
□	0.0.127.in-addr.arpa.	Mail exchange record (MX)	10 awd3.com.	ENG-AUS-NET-826
□	0.0.127.in-addr.arpa.	Host (AAAA)	4321:0:1:2:3:4:567:89ac	ENG-AUS-NET-826
□	1.0.0.127.in-addr.arpa.	Pointer record (PTR)	whatever.0.0.127.in-addr.arpa.	ENG-AUS-NET-826
□	122.0.0.127.in-addr.arpa.	Pointer record (PTR)	qwe.	ENG-AUS-NET-826
□	124.0.0.127.in-addr.arpa.	Pointer record (PTR)	witam.com.pl.	ENG-AUS-NET-826
□	15.0.0.127.in-addr.arpa.	Pointer record (PTR)	mple.microsoft.com.	ENG-AUS-NET-826
□	2.0.0.127.in-addr.arpa.	Pointer record (PTR)	adawd.e.com.	ENG-AUS-NET-826
□	2.0.0.127.in-addr.arpa.	Pointer record (PTR)	someHostNew.0.0.127.in-addr.arpa.	ENG-AUS-NET-826

‹ 1 2 3 4 5 › 1-10 of 46 10

Edit DNS records

1. Go to My Dashboard > DHCP & DNS Management.
2. Click on DNS Zones and use the filters on the left to find the required zone if necessary.



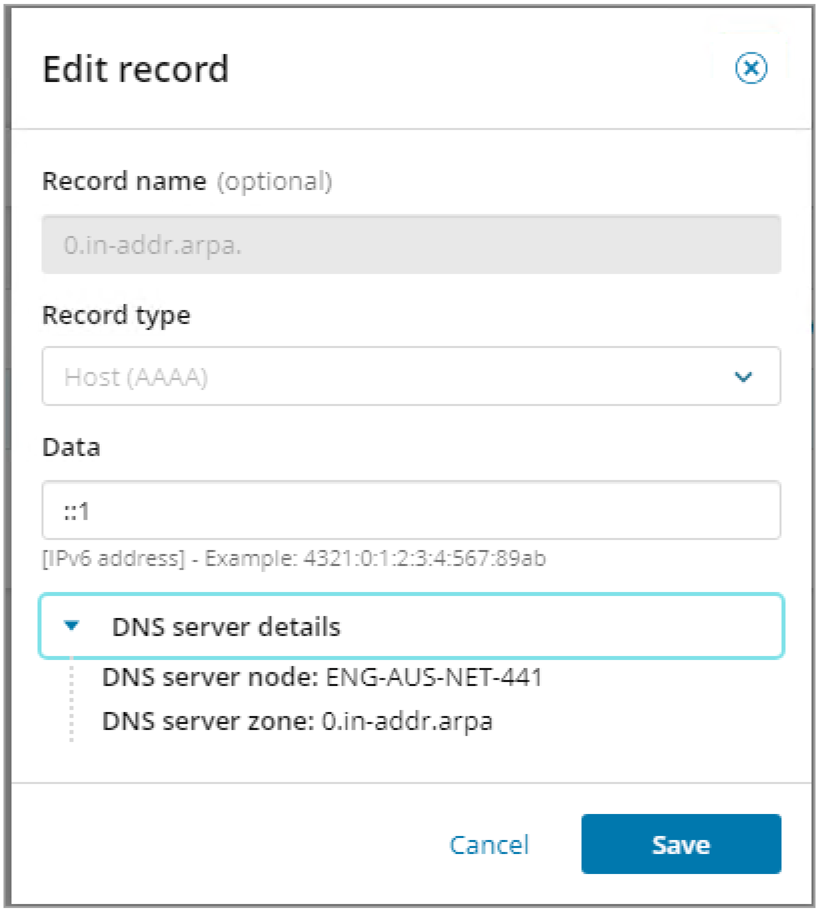
Lookup Type
- ☑ Forward 5
- □ Reverse 5

Server Name
- ☑ ENG-AUS-NET-849 5

Server Type
- □ Bind 5

□	Zone name	View name	Zone status	Zone type	Lookup type	DNS server	Server type	IP address
□	hl.local		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	IPAM1594test		Up	Stub	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	localhost		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	localhost.localdomain		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	testsZone		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85

3. Select the required zone and then click DNS Records. The DNS Records details page for this zone is displayed.
4. Select a single record, and click Edit.



Edit record

Record name (optional)

0.in-addr.arpa.

Record type

Host (AAAA)

Data

::1

[IPv6 address] - Example: 4321:0:1:2:3:4:567:89ab

DNS server details

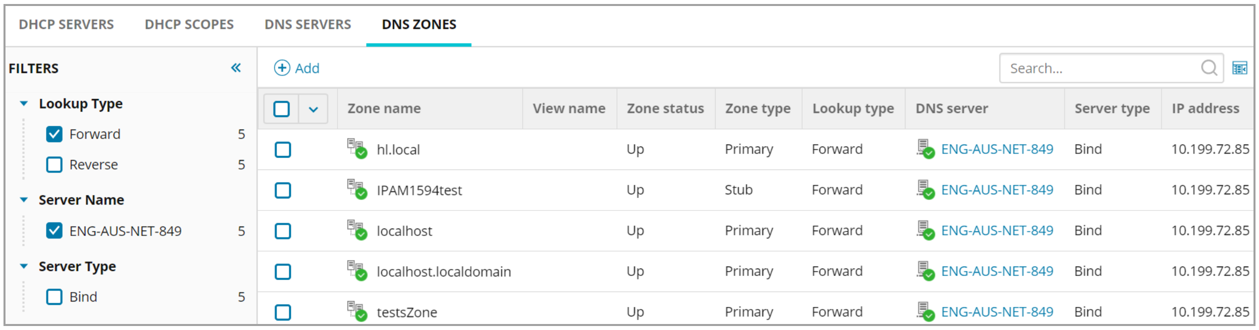
DNS server node: ENG-AUS-NET-441

DNS server zone: 0.in-addr.arpa

5. Update the Data fields as appropriate.

Add a DNS record

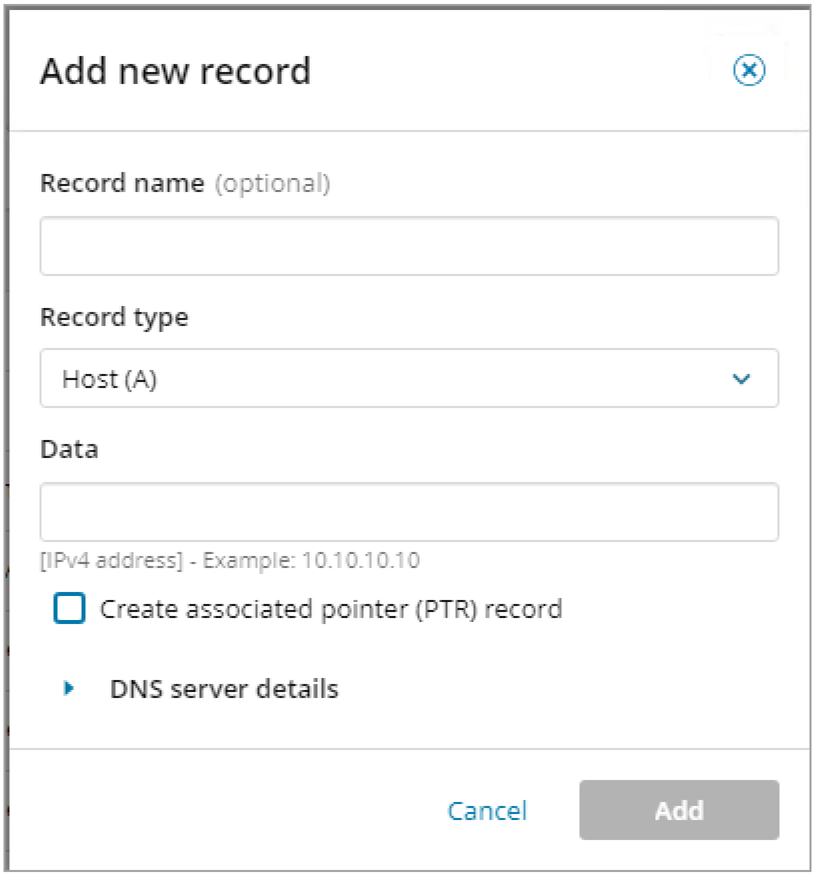
1. Go to My Dashboard > DHCP & DNS Management.
2. Click on DNS Zones and use the filters on the left to find the required zone.



- Lookup Type
  - ☑ Forward 5
  - □ Reverse 5
- Server Name
  - ☑ ENG-AUS-NET-849 5
- Server Type
  - □ Bind 5

□	Zone name	View name	Zone status	Zone type	Lookup type	DNS server	Server type	IP address
□	hl.local		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	IPAM1594test		Up	Stub	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	localhost		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	localhost.localdomain		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85
□	testsZone		Up	Primary	Forward	ENG-AUS-NET-849	Bind	10.199.72.85

3. Select the required zone and then click DNS Records. The DNS Records details page for this zone is displayed.
4. Click Add. The Add new record window is displayed.



Add new record

Record name (optional)

Record type: Host (A)

Data

[IPv4 address] - Example: 10.10.10.10

□ Create associated pointer (PTR) record

5. Enter a record name, select the record type, and enter the appropriate data:
6.

Host (A)	IPv4 Address record	Enter the IPv4 address, and check the box if you want to create an associated pointer (PTR) record.
Host (AAAA)	IPv6 address record	Enter the IPv6 address
Alias (CNAME)	Canonical name record	Enter the canonical name.
Mail exchange record (MX)	Mail exchange record	Enter the mail exchange domain name.
Pointer record (PTR)	PTR resource record	Enter the targeted domain name.

7. Click Add to add your record.

DNS Records Mismatch

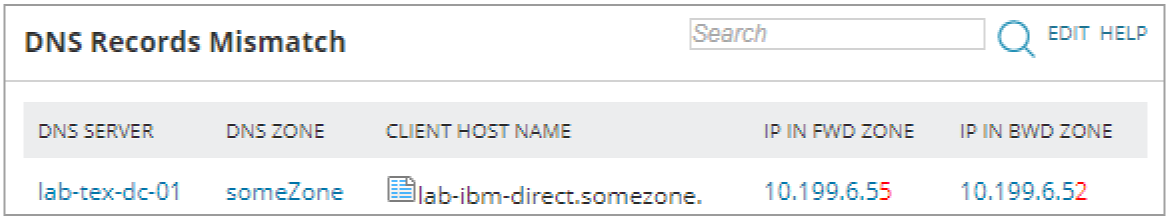
The DNS Records Mismatch widget shows mismatches between host (A) records and Pointer (PTR) records in the same DNS zone. For example, if there was an A record stating:

```
lab-ibm-direct.somezone. IN A 10.199.6.55
```

And a PTR record stating:

```
52.6.199.10-in-addr arpa IN PTR lab-ibm-direct.somezone.
```

This mismatch would result in the following line being displayed in the DNS records mismatch widget:



DNS SERVER	DNS ZONE	CLIENT HOST NAME	IP IN FWD ZONE	IP IN BWD ZONE
lab-tex-dc-01	someZone	lab-ibm-direct.somezone.	10.199.6.55	10.199.6.52

The inconsistencies are displayed in red.

Click Edit to:

- Change the widget title and subtitle.

Edit a DNS server

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management .
2. Select the DNS Server tab.
3. Select the server, and click Edit.

   ⓘ If using the legacy view, click Edit DNS Server.

   The Edit DNS Server windows is displayed for this server.
4. Edit the properties as required, and click Save.

Remove DNS servers in IPAM

1. Go to My Dashboards > DHCP & DNS Management.
2. Select the DNS Servers tab.
3. Select the server and click Delete.

   ⓘ If using the legacy view, click Remove DNS Server.

   The DNS zones that will also be removed when you delete the server are displayed.
   You are given the option to remove zones from the physical DNS Server.
4. Click Delete Listed Items to confirm deletion.

Add a DNS zone

A DNS zone is a contiguous portion of DNS domain namespace over which a DNS server has authority. A DNS server can be authoritative for multiple DNS zones.

A DNS zone contains the resource records for all of the names within that zone. Zone files are used if DNS data is not integrated with Active Directory. If DNS and Active Directory are integrated, then DNS data can be stored in Active Directory.

The following types of DNS Zones are supported in IPAM:

Primary zone	A zone is a primary zone if the DNS server is the authoritative source for all domain in the zone. A primary zone can be stored in Active Directory if the DNS Server is a domain controller.

Secondary zone	A read-only copy of a zone copied from the primary server using zone transfer, used for load balancing and fault tolerance. For more information on Zone transfers, see Understanding zones and zone transfers (© 2019 Microsoft, available at https://docs.microsoft.com, obtained July 29, 2019).
Stub zone	A stub zone is similar to a secondary zone except it contains only those resource records necessary to identify the authoritative Domain Name System (DNS) servers for that zone. For more information, see Understanding stub zones (© 2009 Microsoft, available at https://docs.microsoft.com, obtained July 29, 2019).

There are two kinds of DNS Lookup that can be applied to primary and secondary zones.

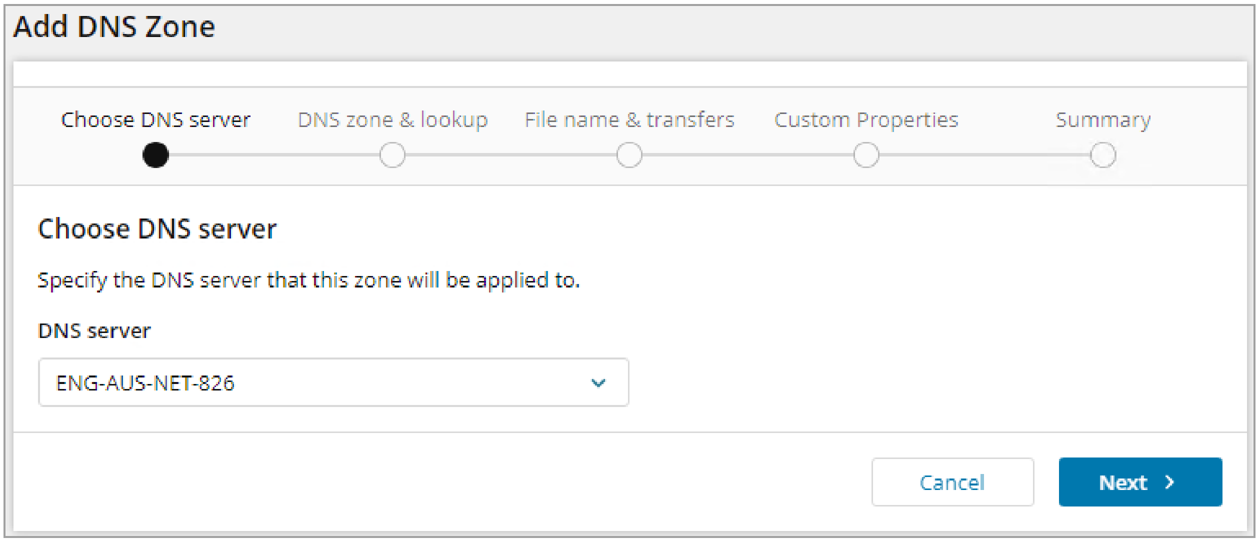
Forward lookup	This is the default. This resolves fully qualified domain names to IP address.
Reverse lookup	Resolves IP addresses to resource names on the network. For more information, see Reverse lookup (© 2019 Microsoft, available at https://docs.microsoft.com, obtained July 29, 2019).

To create a DNS Zone:

1. Go to My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DNS Zones tab, and click Add.

   ⓘ If using the legacy view, you can also select a server on the DNS Server tab and click Add New > DNS Zone.

3. Select the DNS server to which this zone will be applied, and click Next.

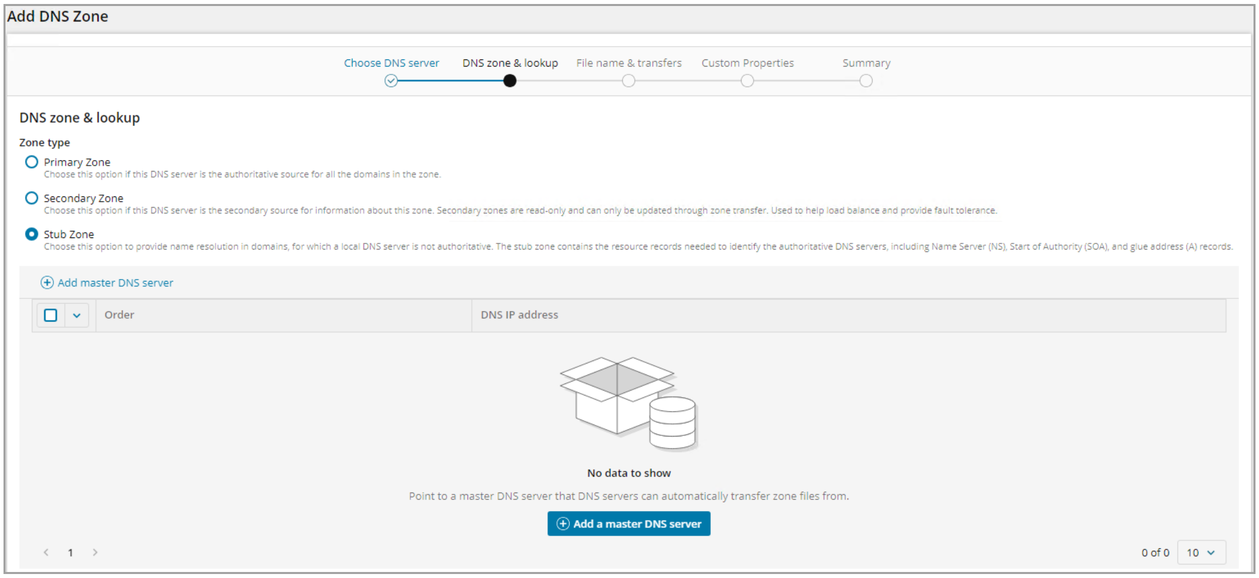

Add DNS Zone

Choose DNS server

Specify the DNS server that this zone will be applied to.

DNS server: ENG-AUS-NET-826

4. Select the zone type.
   - For a Primary zone, you can choose to store the zone in Active Directory if the DNS server is a domain controller.
   - If you select Secondary or Stub, you will need to specify the Master DNS server.



Add DNS Zone

Choose DNS server · DNS zone & lookup · File name & transfers · Custom Properties · Summary

DNS zone & lookup

Zone type

○ Primary Zone
Choose this option if this DNS server is the authoritative source for all the domains in the zone.

○ Secondary Zone
Choose this option if this DNS server is the secondary source for information about this zone. Secondary zones are read-only and can only be updated through zone transfer. Used to help load balance and provide fault tolerance.

● Stub Zone
Choose this option to provide name resolution in domains, for which a local DNS server is not authoritative. The stub zone contains the resource records needed to identify the authoritative DNS servers, including Name Server (NS), Start of Authority (SOA), and glue address (A) records.

⊕ Add master DNS server

□	Order	DNS IP address

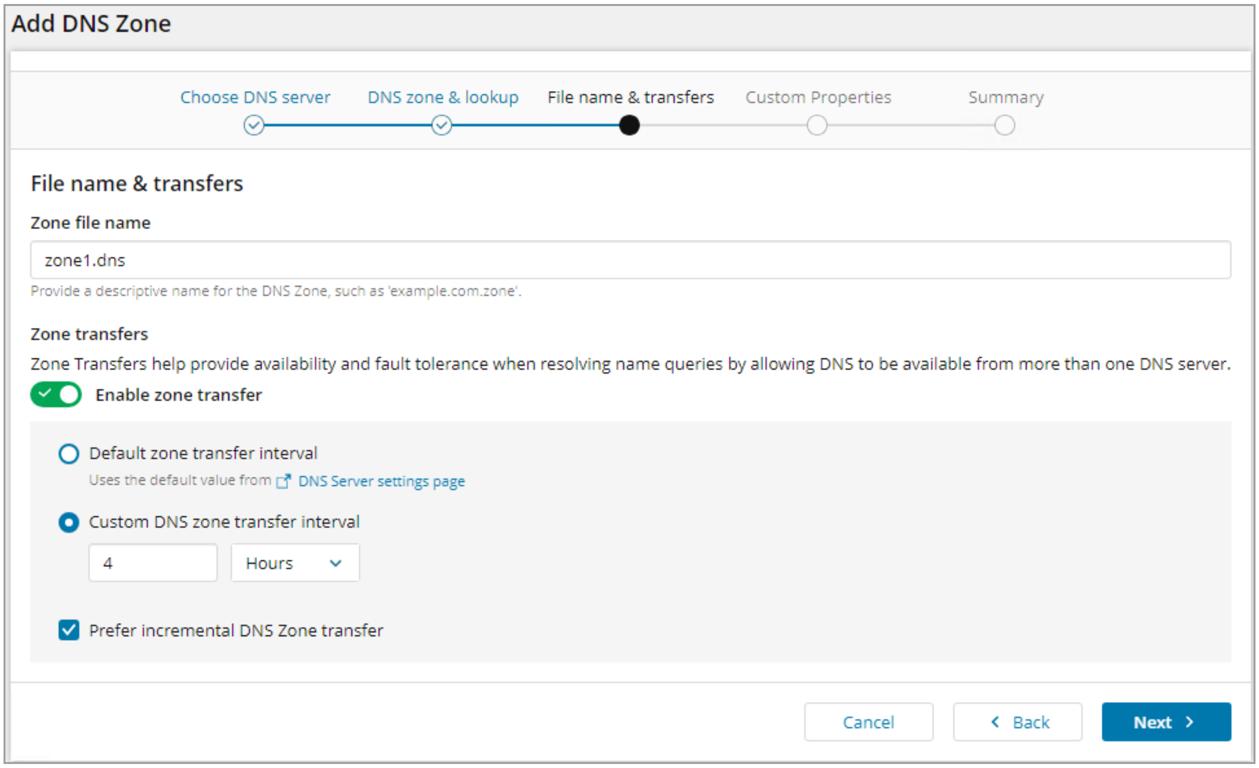
No data to show

Point to a master DNS server that DNS servers can automatically transfer zone files from.

5. Select the DNS Lookup Type:
   - For Forward lookup, enter the name for this DNS Zone.
   - For Reverse lookup, enter the Network ID or Reverse lookup zone name.
6. Click Next.
7. Enter the Zone File Name, or use the default. The zone file is used to store zone data on the DNS server computer. The default is the DNS Zone Name with a .dns extension.
8. If you want to enable Zone Transfers, check Enable Zone Transfer, and either accept the default transfer interval, or enter the interval required.

> Zone transfers are used to keep a secondary or stub DNS zone synchronized with its primary DNS server. You can choose to either perform a full transfer at set intervals or use incremental zone transfers to only pulls the zone changes needed to synchronize the copy of the zone with its source.

9. Click the Custom DNS zone transfer interval, and set the time interval if you want to use this method rather than full transfer of the entire zone database.



Add DNS Zone

File name & transfers

Zone file name

zone1.dns

Provide a descriptive name for the DNS Zone, such as 'example.com.zone'.

Zone transfers

Zone Transfers help provide availability and fault tolerance when resolving name queries by allowing DNS to be available from more than one DNS server.

Enable zone transfer

○ Default zone transfer interval

Uses the default value from DNS Server settings page

● Custom DNS zone transfer interval

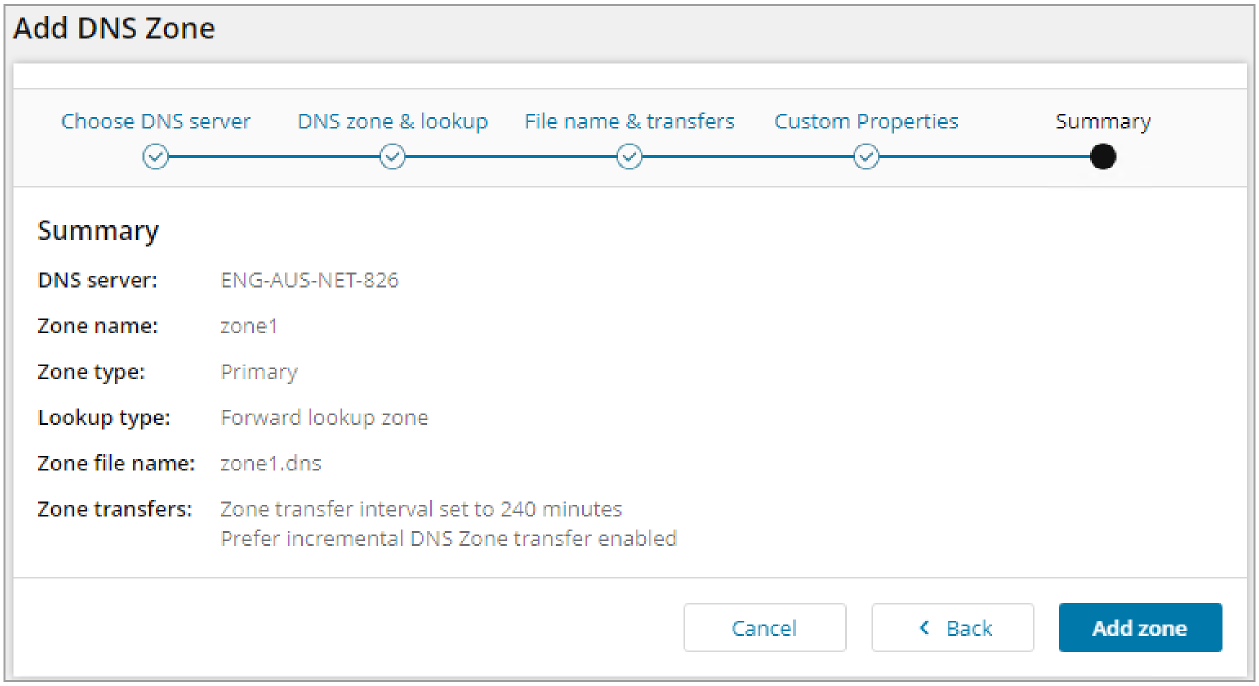
4 Hours

☑ Prefer incremental DNS Zone transfer

10. Click Next.

11. Click Manage Custom Properties to open custom properties settings. Add or import any applicable custom properties. Click Next to continue.

12. Review the information, and click Add zone.



Add DNS Zone

Summary

DNS server: ENG-AUS-NET-826

Zone name: zone1

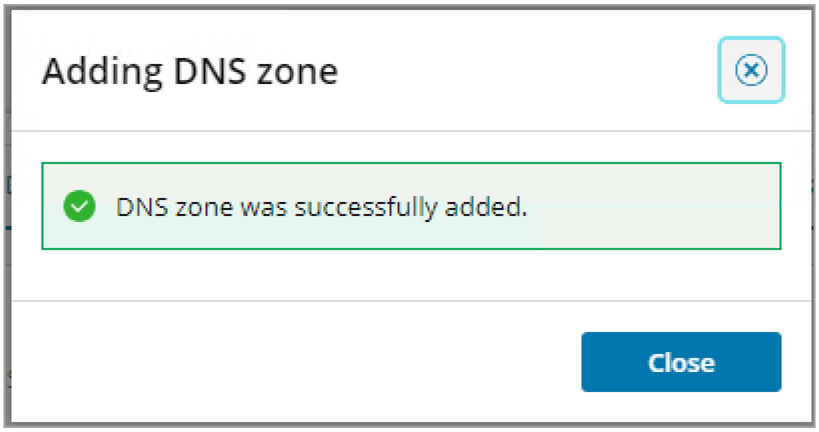
Zone type: Primary

Lookup type: Forward lookup zone

Zone file name: zone1.dns

Zone transfers: Zone transfer interval set to 240 minutes
Prefer incremental DNS Zone transfer enabled

13. Click Close.



Adding DNS zone

DNS zone was successfully added.

Edit a DNS zone

1. Go to My Dashboards > DHCP & DNS Management.
2. Click the DNS Zones tab.
3. Select a zone to edit.
4. Click Edit.

   If using the legacy view, click Edit Zone Details.

5. Edit the zone type, the DNS file name, and transfer details as required.
6. Review the details and click Update Zone.

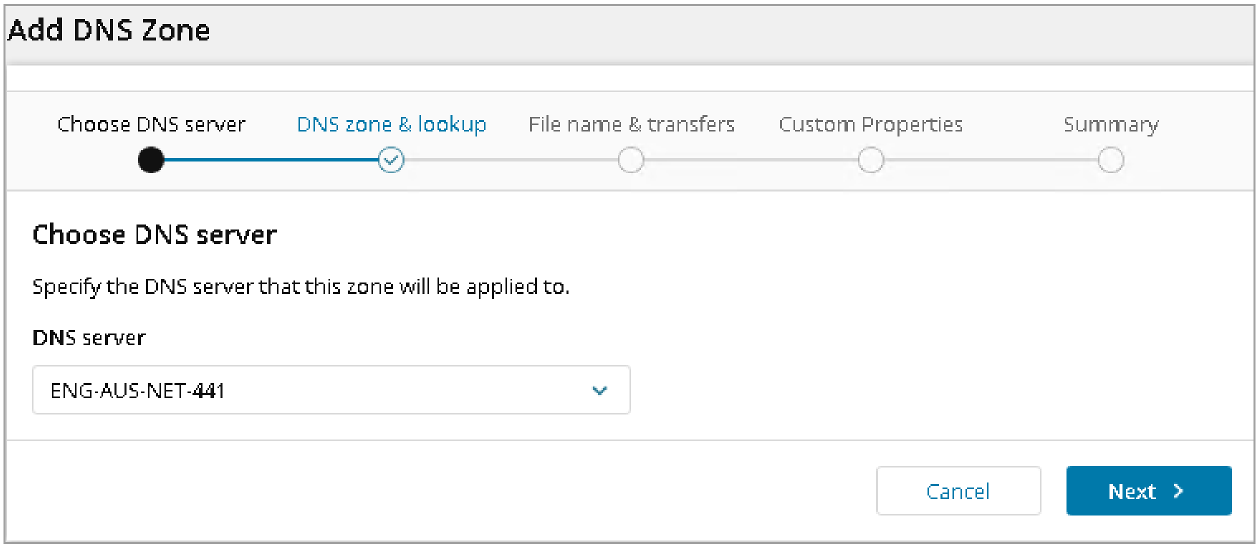
DNS secondary zones and zone transfers

DNS zones should be available on more than one DNS server to ensure availability. If a zone is only available on one server, name queries for that zone will fail if the server goes down or is otherwise unreachable. To ensure the information in the secondary zone remains synchronized with the primary zone, you can specify the frequency of polls and use incremental zone transfers.

Set up a secondary DNS zone

1. From the DHCP & DNS Management screen, select DNS Zones and click Add.

   The Add DNS Zone window is displayed.



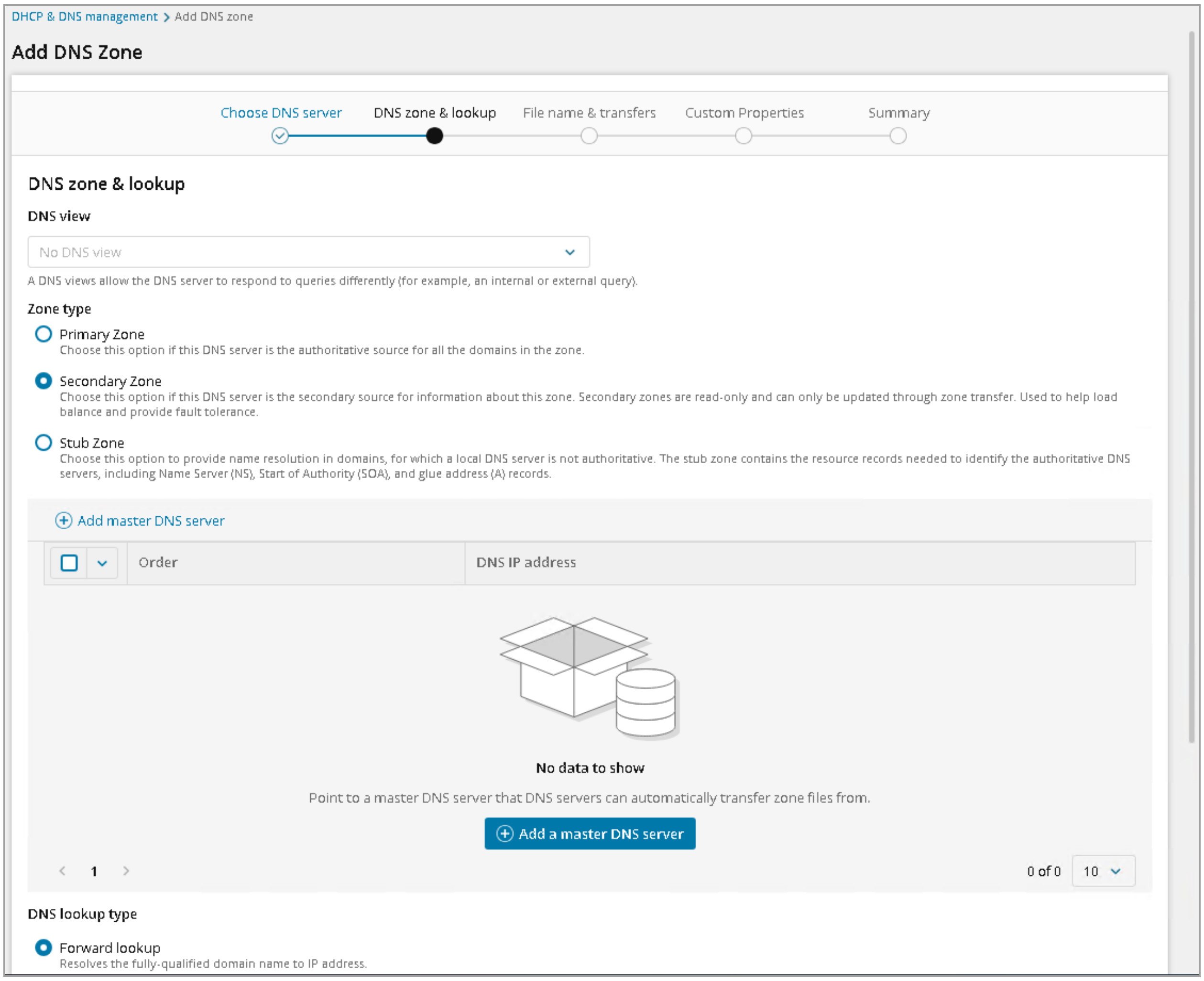
Add DNS Zone

Choose DNS server

Specify the DNS server that this zone will be applied to.

DNS server: ENG-AUS-NET-441

2. Select the server that the secondary DNS Zone (see warning below) should be applied to, and click Next.
3. The DNS Zone & Lookup tab is displayed.



DHCP & DNS management > Add DNS zone

Add DNS Zone

DNS zone & lookup

DNS view

No DNS view

A DNS views allow the DNS server to respond to queries differently (for example, an internal or external query).

Zone type

○ Primary Zone
Choose this option if this DNS server is the authoritative source for all the domains in the zone.

● Secondary Zone
Choose this option if this DNS server is the secondary source for information about this zone. Secondary zones are read-only and can only be updated through zone transfer. Used to help load balance and provide fault tolerance.

○ Stub Zone
Choose this option to provide name resolution in domains, for which a local DNS server is not authoritative. The stub zone contains the resource records needed to identify the authoritative DNS servers, including Name Server (NS), Start of Authority (SOA), and glue address (A) records.

No data to show

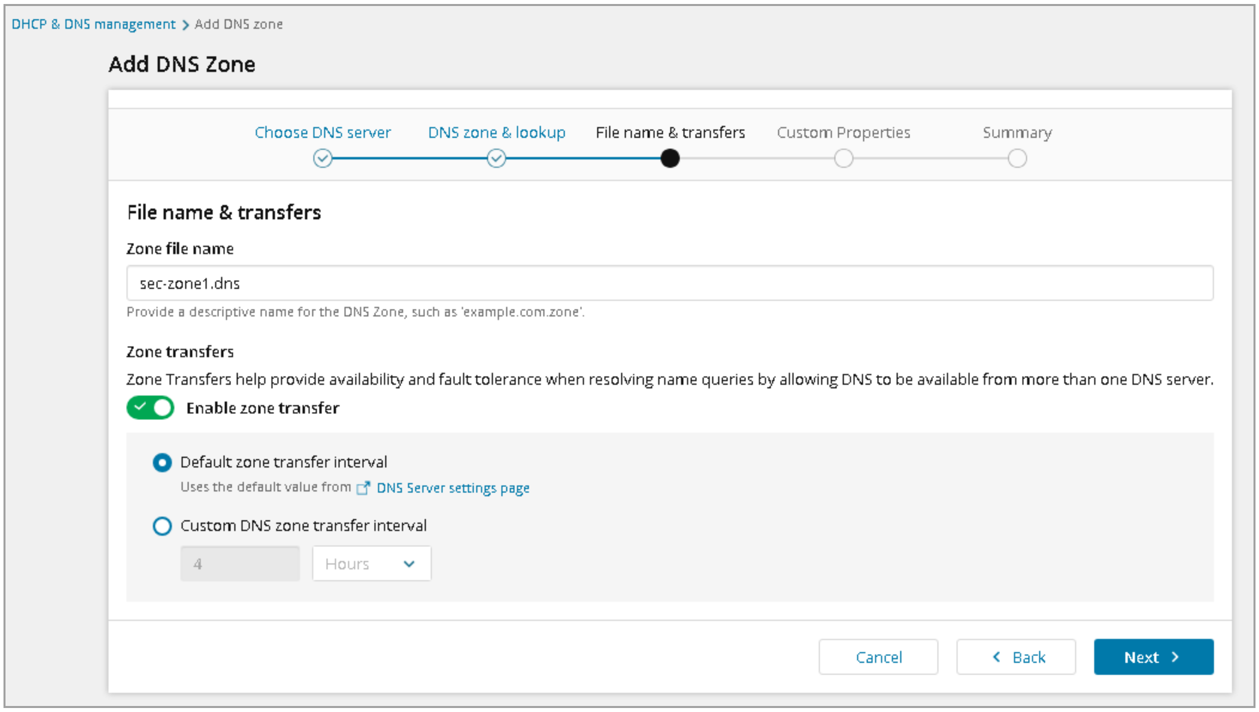
Point to a master DNS server that DNS servers can automatically transfer zone files from.

DNS lookup type

● Forward lookup
Resolves the fully-qualified domain name to IP address.

4. Click Add Master DNS Server and enter the URL for the primary DNS zone.
5. Select the lookup type for the secondary zone, enter a name for it, and click Next.

   The File Name & Transfer tab is displayed.



File name & transfers

Zone file name

sec-zone1.dns

Provide a descriptive name for the DNS Zone, such as 'example.com.zone'.

Zone transfers

Zone Transfers help provide availability and fault tolerance when resolving name queries by allowing DNS to be available from more than one DNS server.

☑ Enable zone transfer

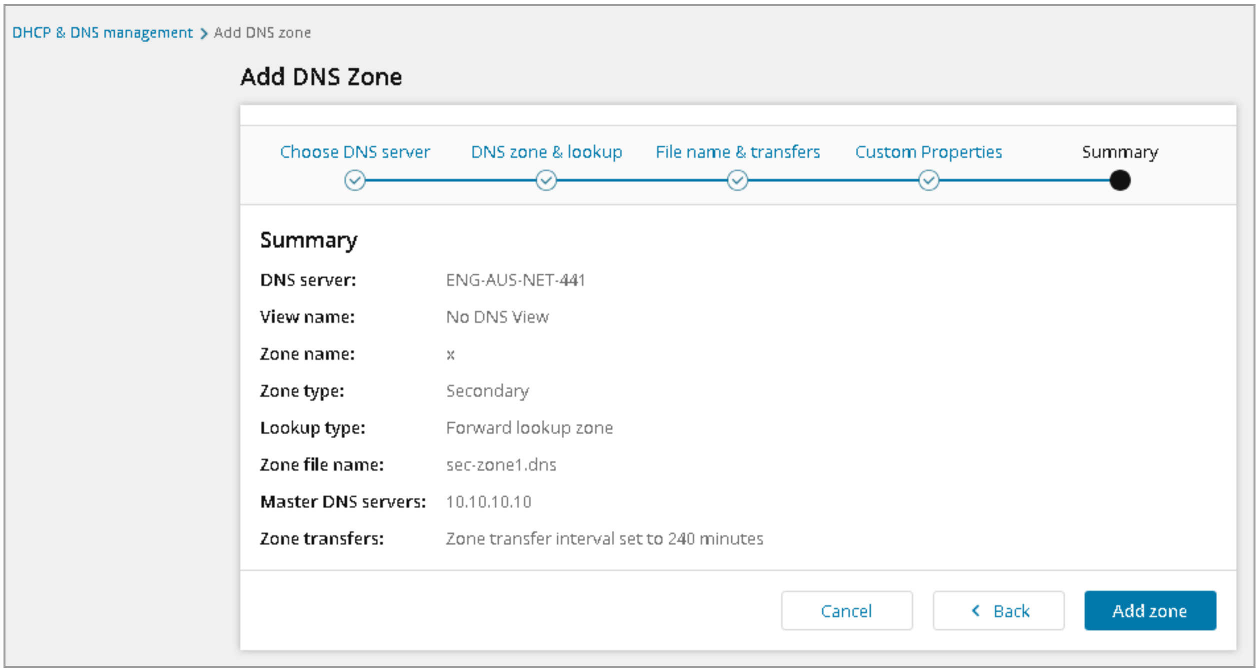
● Default zone transfer interval

Uses the default value from DNS Server settings page

○ Custom DNS zone transfer interval

4 Hours

6. Check the Enable Zone Transfer box, and either select to use the default zone transfer interval (inherited from the primary DNS Server settings) or enter a specific value here.
7. Click Manage custom properties to add any custom properties. Click Next.
8. Verify the details displayed, and then click Add zone.

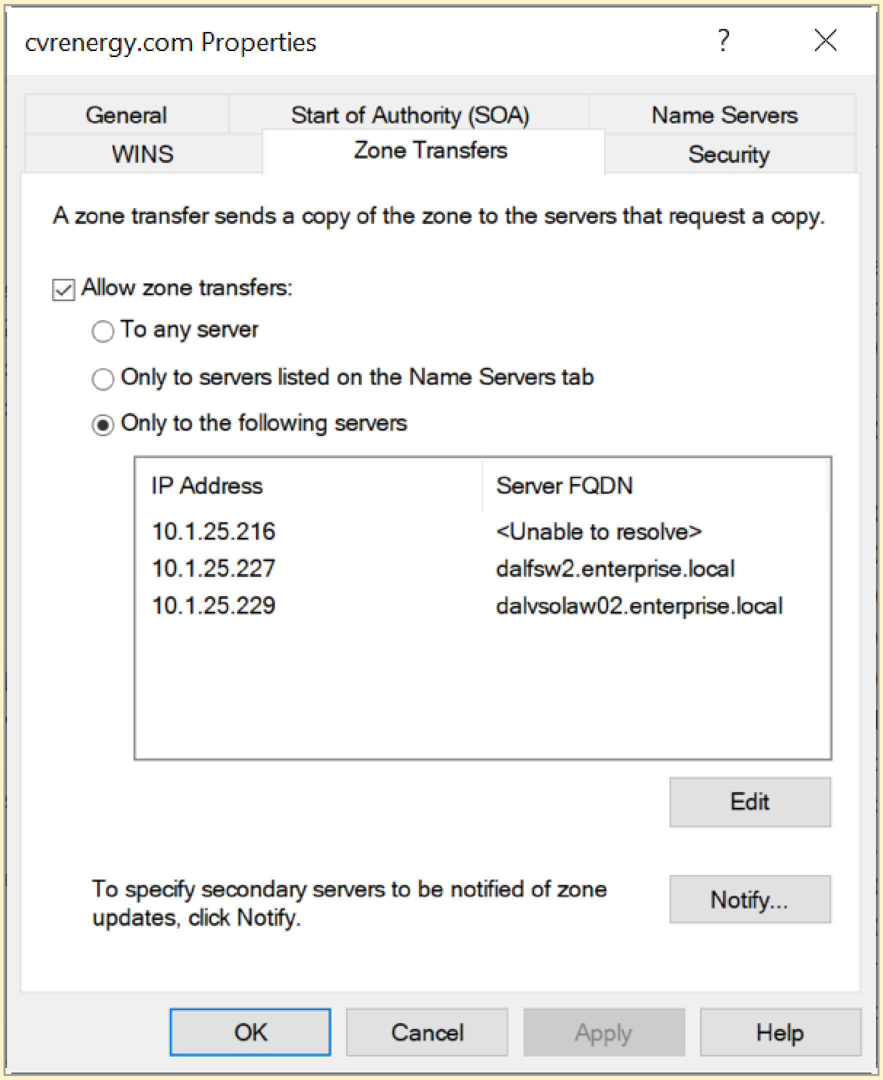


Summary

DNS server:	ENG-AUS-NET-441
View name:	No DNS View
Zone name:	x
Zone type:	Secondary
Lookup type:	Forward lookup zone
Zone file name:	sec-zone1.dns
Master DNS servers:	10.10.10.10
Zone transfers:	Zone transfer interval set to 240 minutes

The secondary zone is created.

Warning: IPAM uses the DNS Zone Transfer mechanism to get information about DNS records. To achieve this on Windows servers, IPAM poller must be added to the list of servers allowed for zone transfer. This results in IPAM automatically switching the Windows Server setting to "Only to following servers" upon every scan. This means only secondary DNS Zones that are on the servers in the "following servers" list are updated.


cvrenergy.com Properties

A zone transfer sends a copy of the zone to the servers that request a copy.

☑ Allow zone transfers:

○ To any server

○ Only to servers listed on the Name Servers tab

● Only to the following servers

IP Address	Server FQDN
10.1.25.216	<Unable to resolve>
10.1.25.227	dalfsw2.enterprise.local
10.1.25.229	dalvsolaw02.enterprise.local

To specify secondary servers to be notified of zone updates, click Notify.

Therefore you must ensure that the servers on which you want to create Secondary Zones are included in the list.

Monitor the Infoblox environment

Requirements

Infoblox servers have to be added as SolarWinds nodes and monitored by SolarWinds (Polling Method cannot be set to External Node).

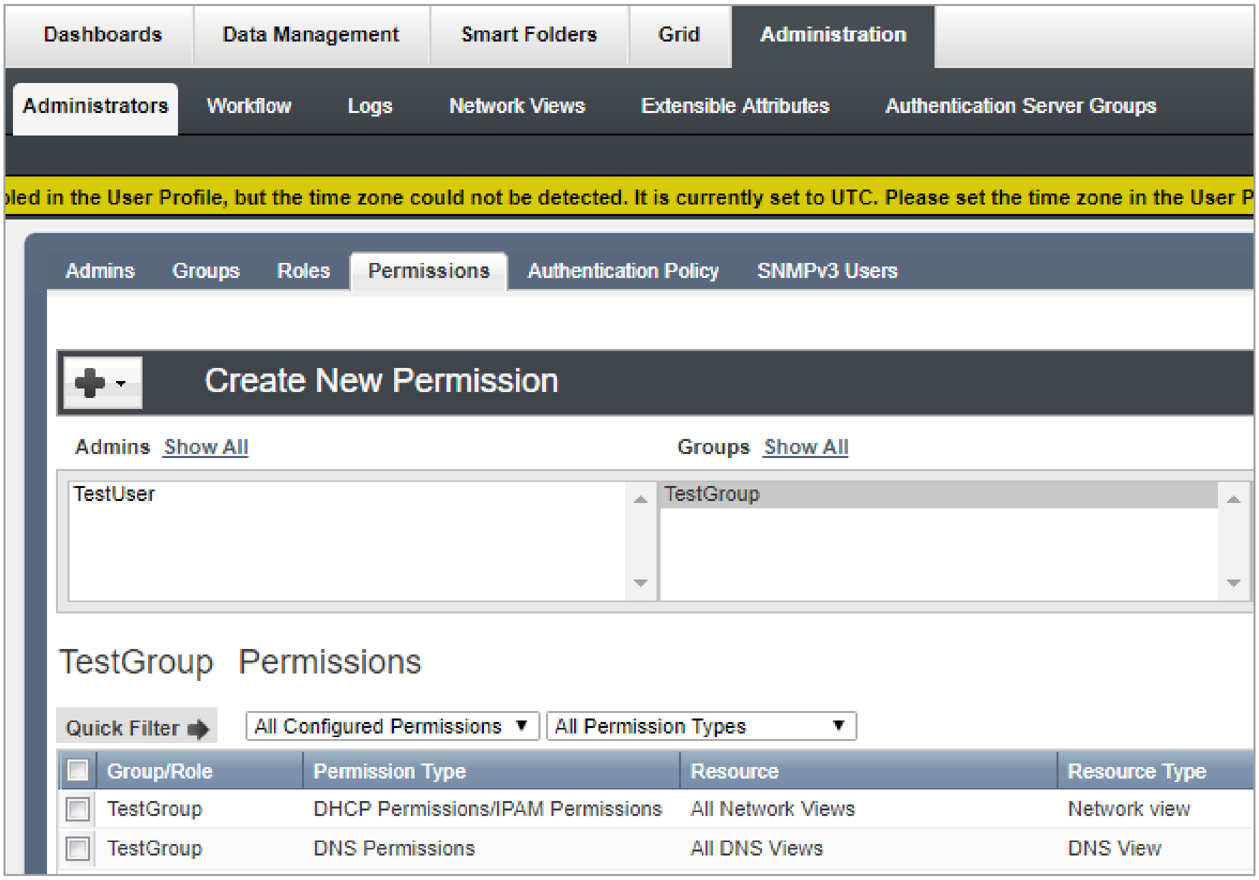
Infoblox servers have to support wAPI v2.5 (wAPI of Infoblox is backward compatible).

The user needs to have following permissions on Infoblox servers:

- MEMBER_DHCP_PROPERTIES
- MEMBER_DNS_PROPERTIES

To set permissions:

1. Go to the Infoblox Management UI.
2. Navigate to Administration > Administration > Permissions.
3. Select the user or group used by IPAM to connect with Infoblox.
4. Add read only (RO) permissions for:
    - `DHCP Permissions/IPAM Permissions` (for resource type Network View)
    - `DNS Permissions` (for resource type DNS View)



bled in the User Profile, but the time zone could not be detected. It is currently set to UTC. Please set the time zone in the User P

Admins Show All: TestUser

Groups Show All: TestGroup

TestGroup Permissions

□	Group/Role	Permission Type	Resource	Resource Type
□	TestGroup	DHCP Permissions/IPAM Permissions	All Network Views	Network view
□	TestGroup	DNS Permissions	All DNS Views	DNS View

Known limitations

Scanning and monitoring of Infoblox DNS and DHCP server is performed in the same way as with other types of DHCP/DNS servers in IPAM, except that it is read only. This means there is no way to modify any settings on the Infoblox server from the IPAM interface. Therefore the following operations are **not** available:

- Edit DHCP Scope details (name, address range, options)
- Set a lease time for scopes
- Set reservations for IP address managed by Infoblox directly in IPAM
- Edit details of DNS zones
- Add new DNS records into DNS zone managed by Infoblox DNS server
- Remove scopes on server when removing server monitored in IPAM
- Remove DNS zones from Infoblox Server when removing DNS server from IPAM
- Monitoring of IPv6 is not available in this release

Integrate IPAM with VMware

IPAM 4.6 introduced integration with VMware® vRealize Orchestrator (vRO). You can use the vRO plug-in to:

- Automate the IP address provisioning process
- Automate DNS updates

The plug-in is available from the IPAM Settings page, and includes over a dozen workflows and actions that you can leverage to script or seamlessly integrate with vRealize Automation (vRA).

The IPAM plug-in supports vCenter Server 6.5, vRealize Orchestrator 7.2, and vRealize Automation 7.2 implementations.

For information, see:

Integrate IPAM with VMware vRealize Orchestrator

vRealize Orchestrator is a workflow tool that automates tasks in a VMware vSphere infrastructure. You can run or script over a dozen different IPAM actions, such as:

- Add or remove a DNS "A" records for an IP address
- Create or remove an IP address reservation on a DHCP server
- Change IP node status, and more

This version of IP Address Manager is compatible with the following VMware products:

- vCenter Server 6.5
- vRealize Orchestrator 7.2
- vRealize Automation 7.2

Adding IPAM support to vRealize Orchestrator is an easy two-step process:

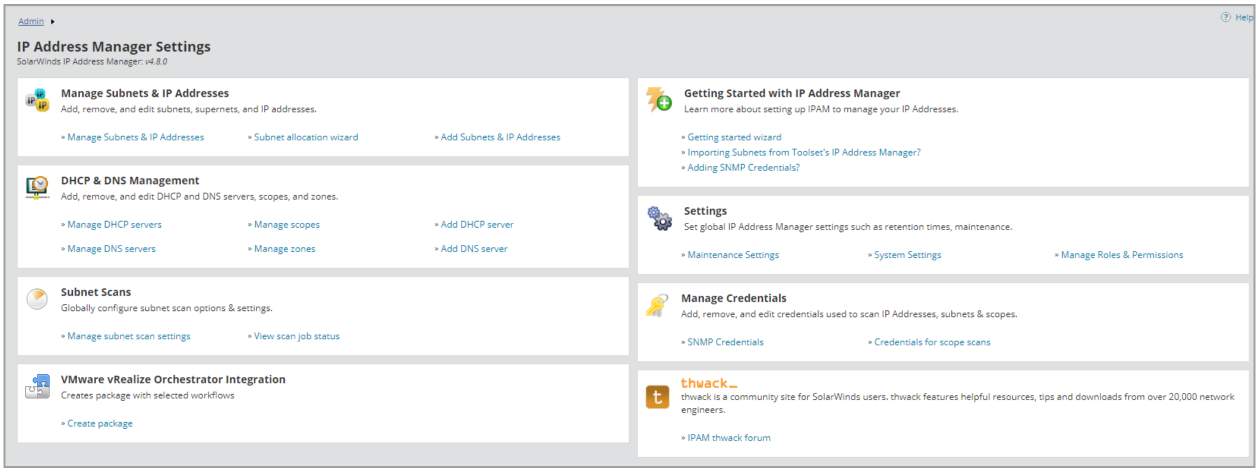
1. Import the VMO package for IPAM (`com.solarwinds.ipam.package`) into vRealize Orchestrator.
2. Run the "Add IPAM host" workflow. The workflow prompts you to enter host properties, proxy settings, and authentication details.

For details, see the following sections.

Import the IPAM package into Orchestrator

1. Open the SolarWinds Web Console and choose Settings > All Settings > IPAM Settings.

   The IP Address Manager Settings page opens.

   Admin ▸

   IP Address Manager Settings

   SolarWinds IP Address Manager: *v4.8.0*

   Manage Subnets & IP Addresses

   Add, remove, and edit subnets, supernets, and IP addresses.

   » Manage Subnets & IP Addresses » Subnet allocation wizard » Add Subnets & IP Addresses

   DHCP & DNS Management

   Add, remove, and edit DHCP and DNS servers, scopes, and zones.

   » Manage DHCP servers » Manage scopes » Add DHCP server

   » Manage DNS servers » Manage zones » Add DNS server

   Subnet Scans

   Globally configure subnet scan options & settings.

   » Manage subnet scan settings » View scan job status

   VMware vRealize Orchestrator Integration

   Creates package with selected workflows

   » Create package

   Getting Started with IP Address Manager

   Learn more about setting up IPAM to manage your IP Addresses.

   » Getting started wizard

   » Importing Subnets from Toolset's IP Address Manager?

   » Adding SNMP Credentials?

   Settings

   Set global IP Address Manager settings such as retention times, maintenance.

   » Maintenance Settings » System Settings » Manage Roles & Permissions

   Manage Credentials

   Add, remove, and edit credentials used to scan IP Addresses, subnets & scopes.

   » SNMP Credentials » Credentials for scope scans

   thwack_

   thwack is a community site for SolarWinds users. thwack features helpful resources, tips and downloads from over 20,000 network engineers.

   » IPAM thwack forum

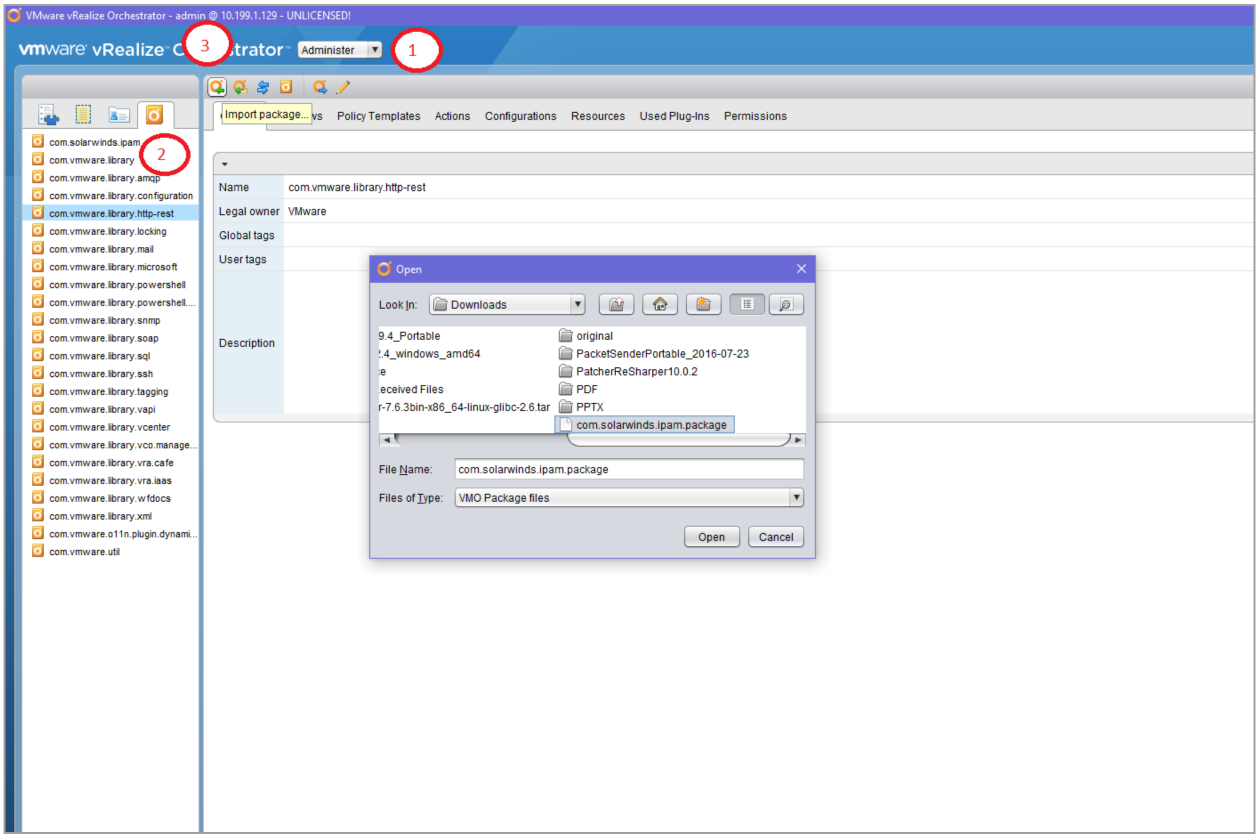
2. In the VMware vRealize Orchestrator Integration section, click Create package.

   The console prompts you to download the `com.solarwinds.ipam.package` file.

3. Download the file to your local system.

4. Open the Orchestrator client and import the package:

   a. Choose the Administer view from the drop-down list on the main menu (see 1 in the following diagram).


VMware vRealize Orchestrator - admin @ 10.199.1.129 - UNLICENSED!
vmware vRealize Orchestrator
Administer
1
2
3
Import package...
Policy Templates
Actions
Configurations
Resources
Used Plug-Ins
Permissions
com.solarwinds.ipam
com.vmware.library
com.vmware.library.amqp
com.vmware.library.configuration
com.vmware.library.http-rest
com.vmware.library.locking
com.vmware.library.mail
com.vmware.library.microsoft
com.vmware.library.powershell
com.vmware.library.powershell...
com.vmware.library.snmp
com.vmware.library.soap
com.vmware.library.sql
com.vmware.library.ssh
com.vmware.library.tagging
com.vmware.library.vapi
com.vmware.library.vcenter
com.vmware.library.vco.manage...
com.vmware.library.vra.cafe
com.vmware.library.vra.iaas
com.vmware.library.wfdocs
com.vmware.library.xml
com.vmware.o11n.plugin.dynami...
com.vmware.util
Open
9.4_Portable
.4_windows_amd64
e
eceived Files
r-7.6.3bin-x86_64-linux-glibc-2.6.tar
original
PacketSenderPortable_2016-07-23
PatcherReSharper10.0.2
PDF
PPTX
com.solarwinds.ipam.package
Open
Cancel

Name: com.vmware.library.http-rest
Legal owner: VMware
Global tags:
User tags:
Description:

Look In: Downloads
File Name: com.solarwinds.ipam.package
Files of Type: VMO Package files

   b. Click the Packages view (see 2 in the above diagram).

   c. Click the Import package icon (see 3 in the above diagram).

   d. Browse to the `com.solarwinds.ipam.package` file that you downloaded and click Open.

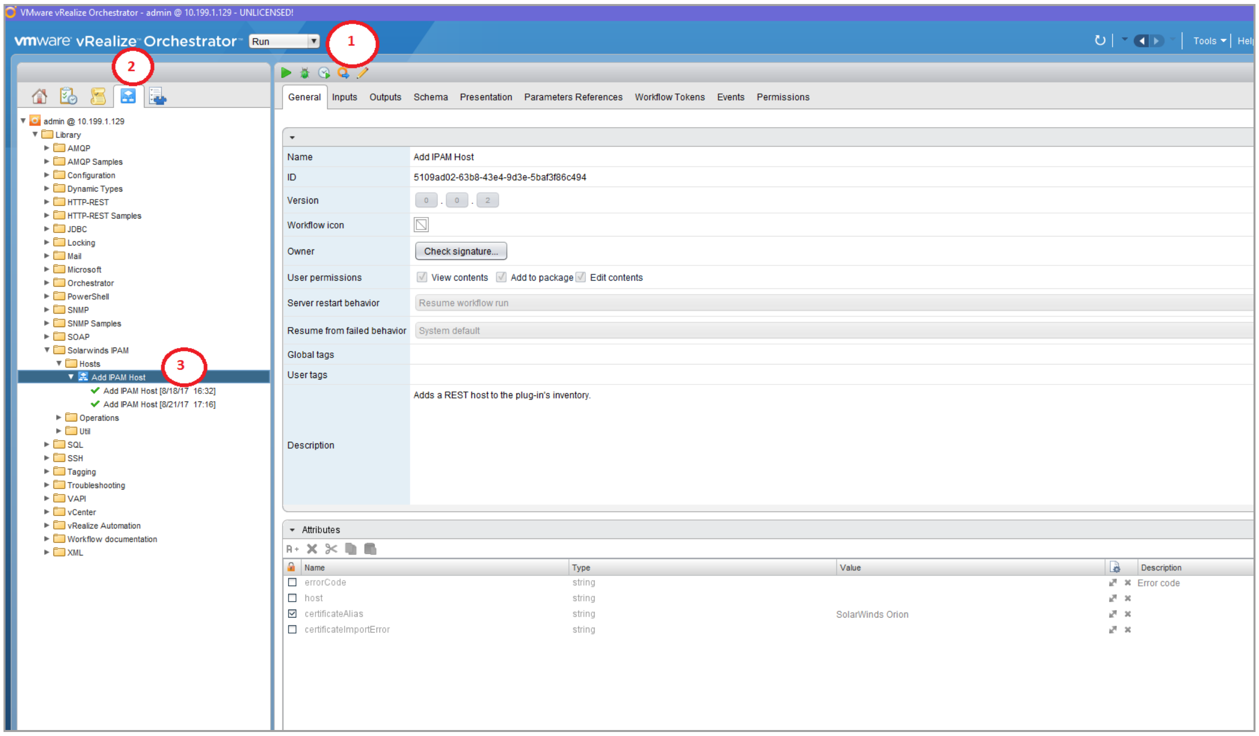
   e. Import the package. Select all of the elements and click Import Selected Elements.

   Orchestrator imports the package.

Run the Add IPAM host workflow to configure the IPAM host

Before you begin, import the IPAM package into Orchestrator using the steps in the previous section.

1. Choose the Run view from the drop-down list on the Orchestrator client main menu (see 1 in the following diagram).



VMware vRealize Orchestrator - admin @ 10.199.1.129 - UNLICENSED!

Name	Add IPAM Host
ID	5109ad02-63b8-43e4-9d3e-5baf3f86c494
Version	0 . 0 . 2
Workflow icon	
Owner	
User permissions	☑ View contents ☑ Add to package ☑ Edit contents
Server restart behavior	Resume workflow run
Resume from failed behavior	System default
Global tags	
User tags	
Description	Adds a REST host to the plug-in's inventory.

	Name	Type	Value	Description
□	errorCode	string		Error code
□	host	string		
☑	certificateAlias	string	SolarWinds Orion	
□	certificateImportError	string		

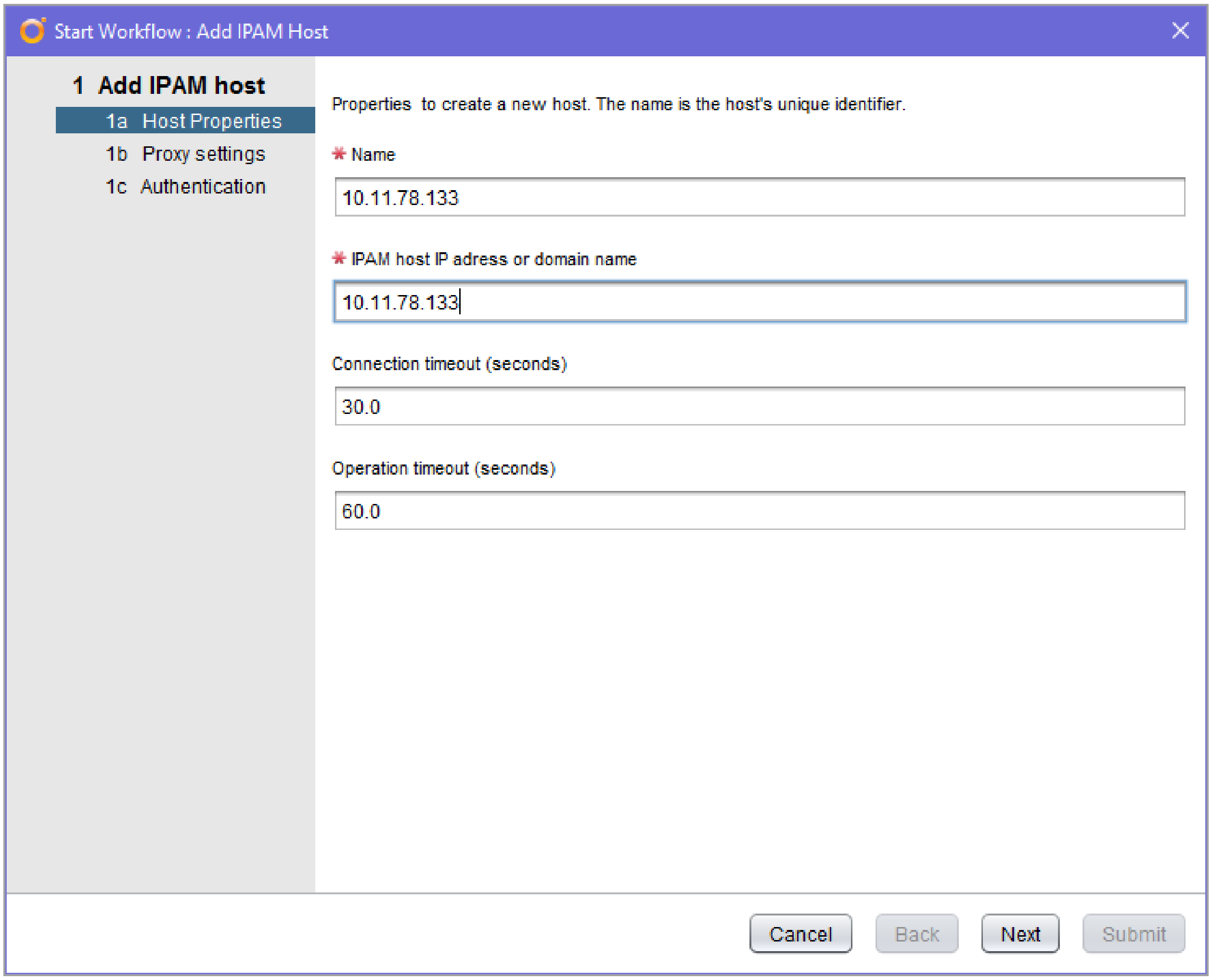
2. Click the Workflows view (see number 2 in the diagram).

3. In the Orchestrator workflow library, navigate to SolarWinds IPAM > Hosts > Add IPAM Host (see number 3 in the diagram).

4. Right-click the Add IPAM Host workflow and select Start workflow.

5. Complete the workflow steps:

   a. Configure the Host Properties screen, and then click Next. The Name should uniquely identify the host.



Start Workflow : Add IPAM Host

1 Add IPAM host

Properties to create a new host. The name is the host's unique identifier.

* Name

10.11.78.133

* IPAM host IP adress or domain name

10.11.78.133

Connection timeout (seconds)

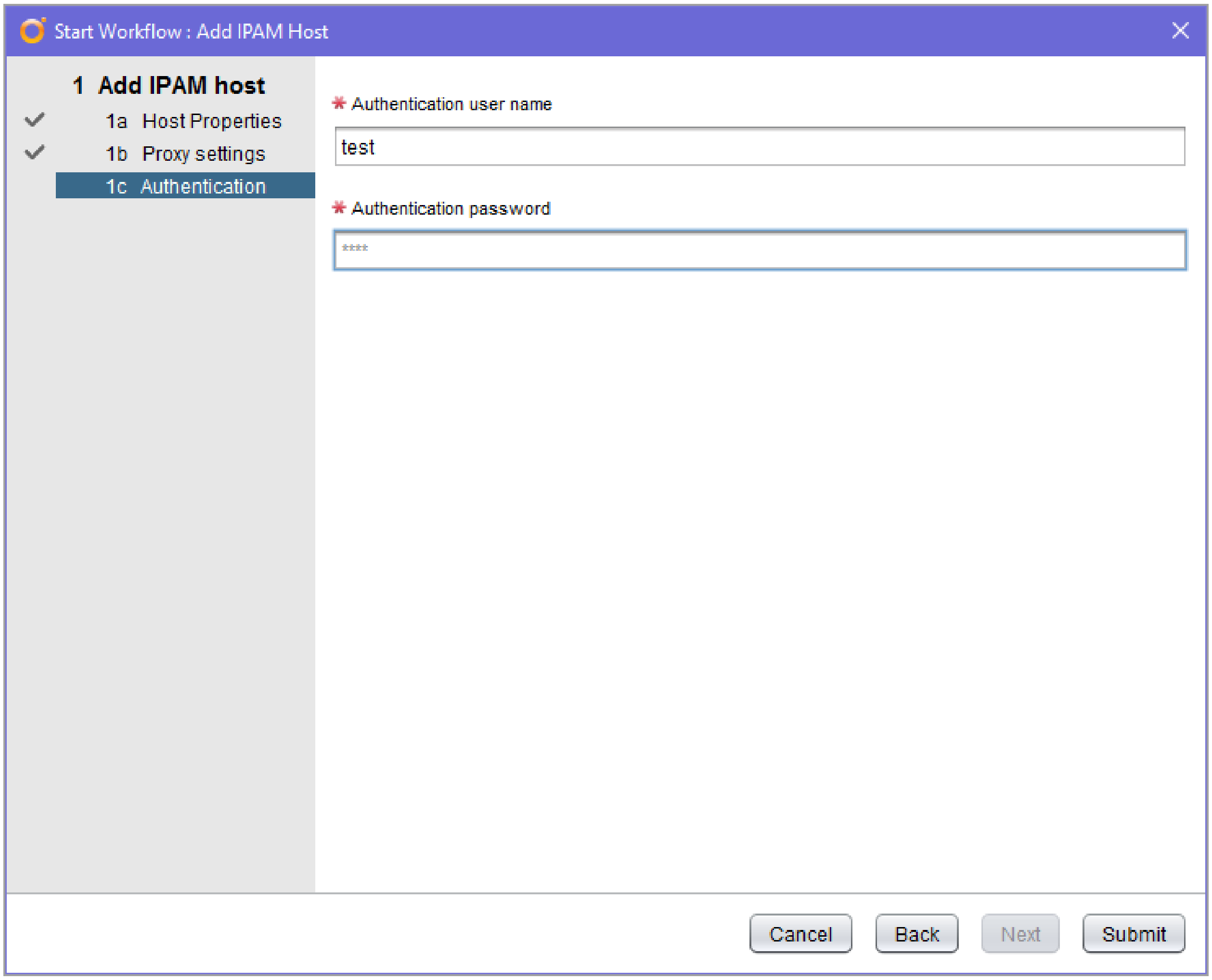
30.0

Operation timeout (seconds)

60.0

   b. (Optional) Configure the Proxy Settings screen, and then click Next.

c. Configure the Authentication screen, and then click Submit. Enter the login credentials for the IPAM host.



* Authentication user name: test

* Authentication password: ****

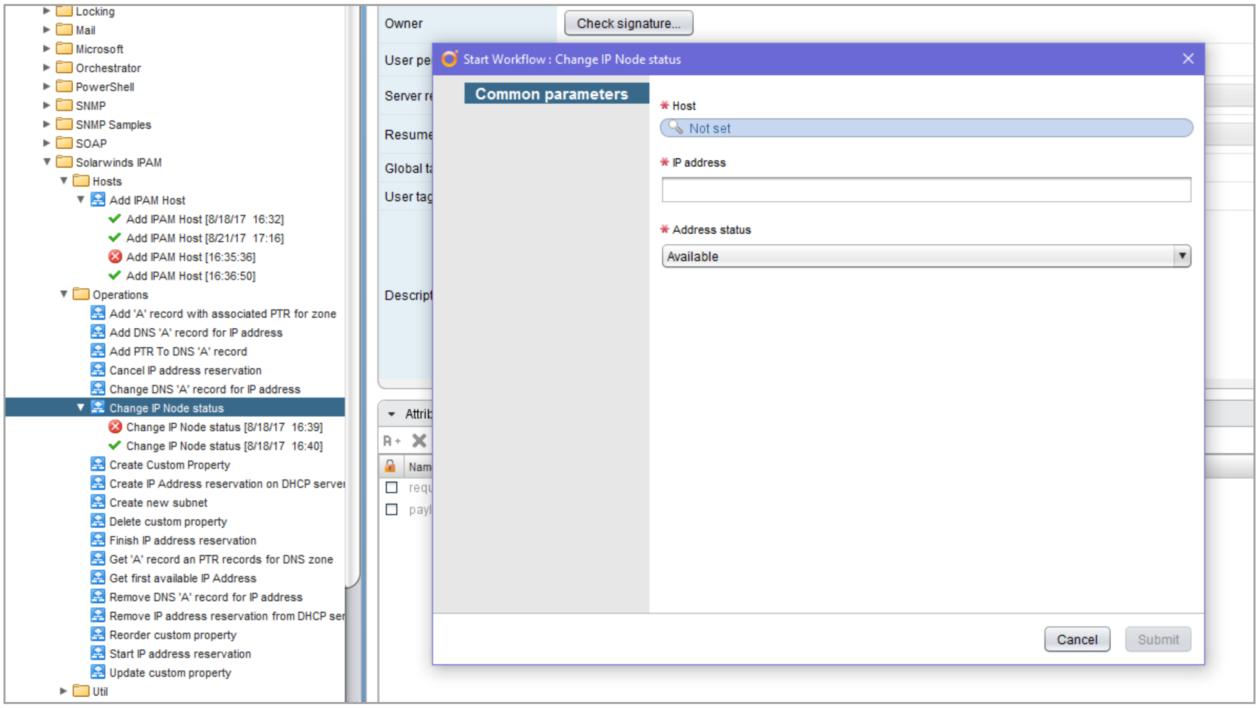
The IPAM host is now configured.

Perform IPAM operations in Orchestrator

Before you begin—Configure the IPAM host using the steps in the previous section.

The following steps demonstrate how to run the Change IP Node Status operation using the Orchestrator client.

1. Choose the Run view from the drop-down list on the Orchestrator client main menu.
2. Click the Workflows view.
3. In the Orchestrator workflow library, navigate to SolarWinds IPAM > Operations.
4. Right-click the "Change IP Node status" workflow and select Start workflow.

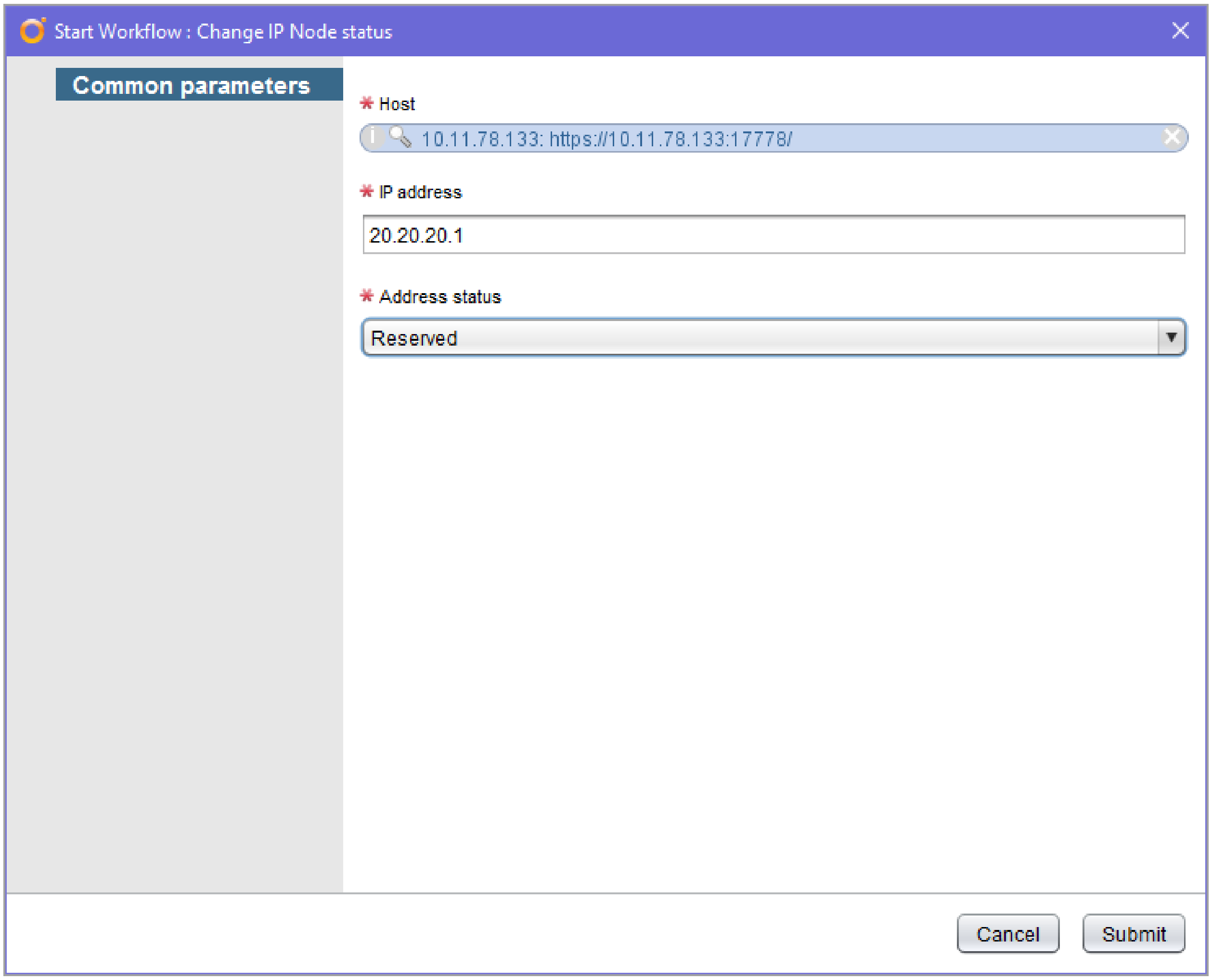

Locking
Mail
Microsoft
Orchestrator
PowerShell
SNMP
SNMP Samples
SOAP
Solarwinds IPAM
Hosts
Add IPAM Host
Add IPAM Host [8/18/17 16:32]
Add IPAM Host [8/21/17 17:16]
Add IPAM Host [16:35:36]
Add IPAM Host [16:36:50]
Operations
Add 'A' record with associated PTR for zone
Add DNS 'A' record for IP address
Add PTR To DNS 'A' record
Cancel IP address reservation
Change DNS 'A' record for IP address
Change IP Node status
Change IP Node status [8/18/17 16:39]
Change IP Node status [8/18/17 16:40]
Create Custom Property
Create IP Address reservation on DHCP server
Create new subnet
Delete custom property
Finish IP address reservation
Get 'A' record an PTR records for DNS zone
Get first available IP Address
Remove DNS 'A' record for IP address
Remove IP address reservation from DHCP ser
Reorder custom property
Start IP address reservation
Update custom property
Util
Owner
Check signature...
User pe
Server re
Resume
Global ta
User tag
Descript
Attrib
Nam
requ
payl
Start Workflow : Change IP Node status
Common parameters
Cancel
Submit

* Host: Not set

* IP address:

* Address status: Available

5. Enter values in the fields and click Submit.

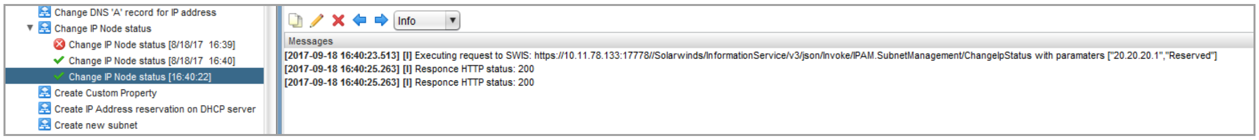


* Host: 10.11.78.133: https://10.11.78.133:17778/

* IP address: 20.20.20.1

* Address status: Reserved

IPAM completes the operation.


Change DNS 'A' record for IP address
Change IP Node status
Change IP Node status [8/18/17 16:39]
Change IP Node status [8/18/17 16:40]
Change IP Node status [16:40:22]
Create Custom Property
Create IP Address reservation on DHCP server
Create new subnet
Info
Messages

```
[2017-09-18 16:40:23.513] [I] Executing request to SWIS: https://10.11.78.133:17778//Solarwinds/InformationService/v3/json/Invoke/IPAM.SubnetManagement/ChangeIpStatus with paramaters ["20.20.20.1","Reserved"]
[2017-09-18 16:40:25.263] [I] Responce HTTP status: 200
[2017-09-18 16:40:25.263] [I] Responce HTTP status: 200
```

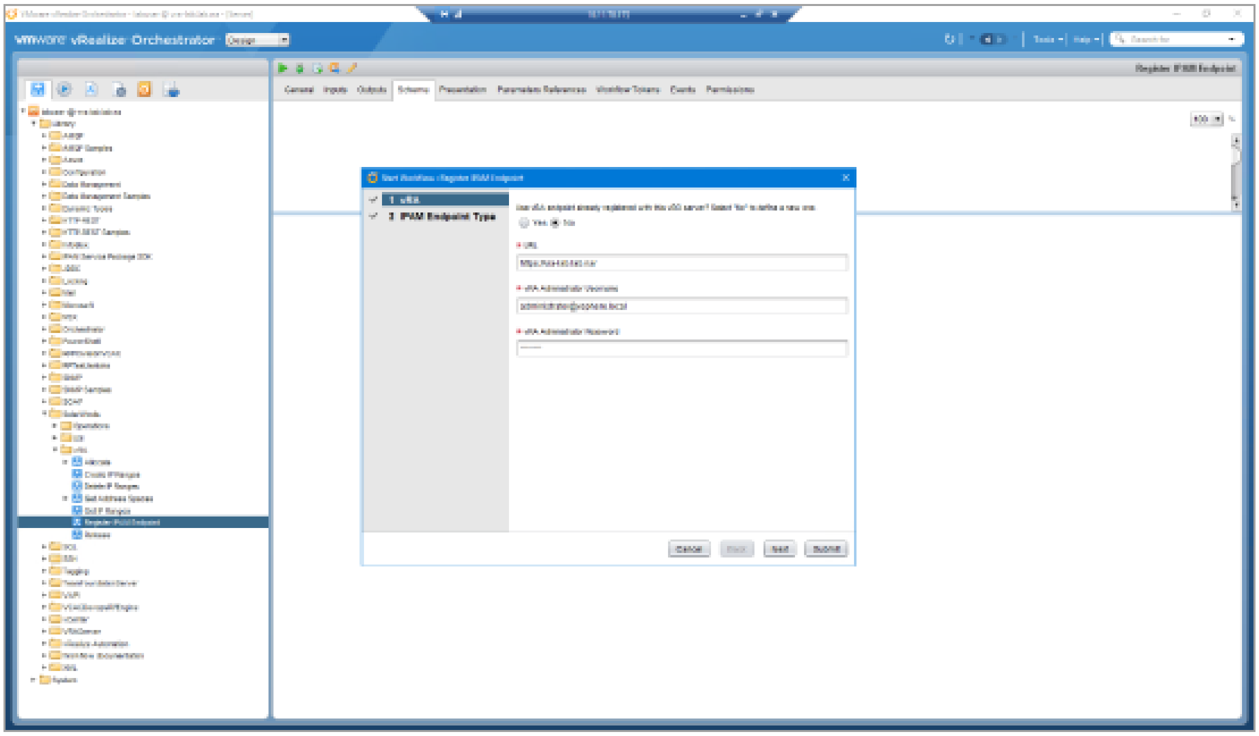
Integrate IPAM with VMware vRealize Automation

See Integrate SolarWinds IPAM with VMware vRealize Orchestrator for information on importing the IPAM package into Orchestrator.

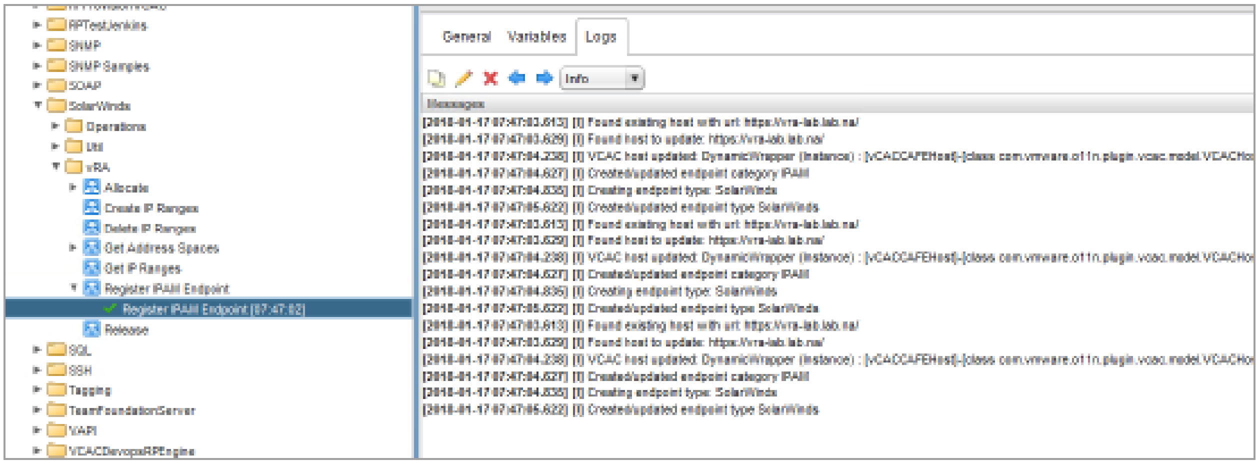
vRealize Automation integration

IPAM Endpoint type

1. Open Design > Workflows > Library > SolarWinds > vRAM, and run Register IPAM Endpoint.
2. Enter the vRA URL, and administrator credentials, and then click Next and Submit.


vmware vRealize Orchestrator
1 vRA
2 IPAM Endpoint Type
Yes
No
URL
vRA Administrator Username
vRA Administrator Password
Cancel
Back
Next
Submit

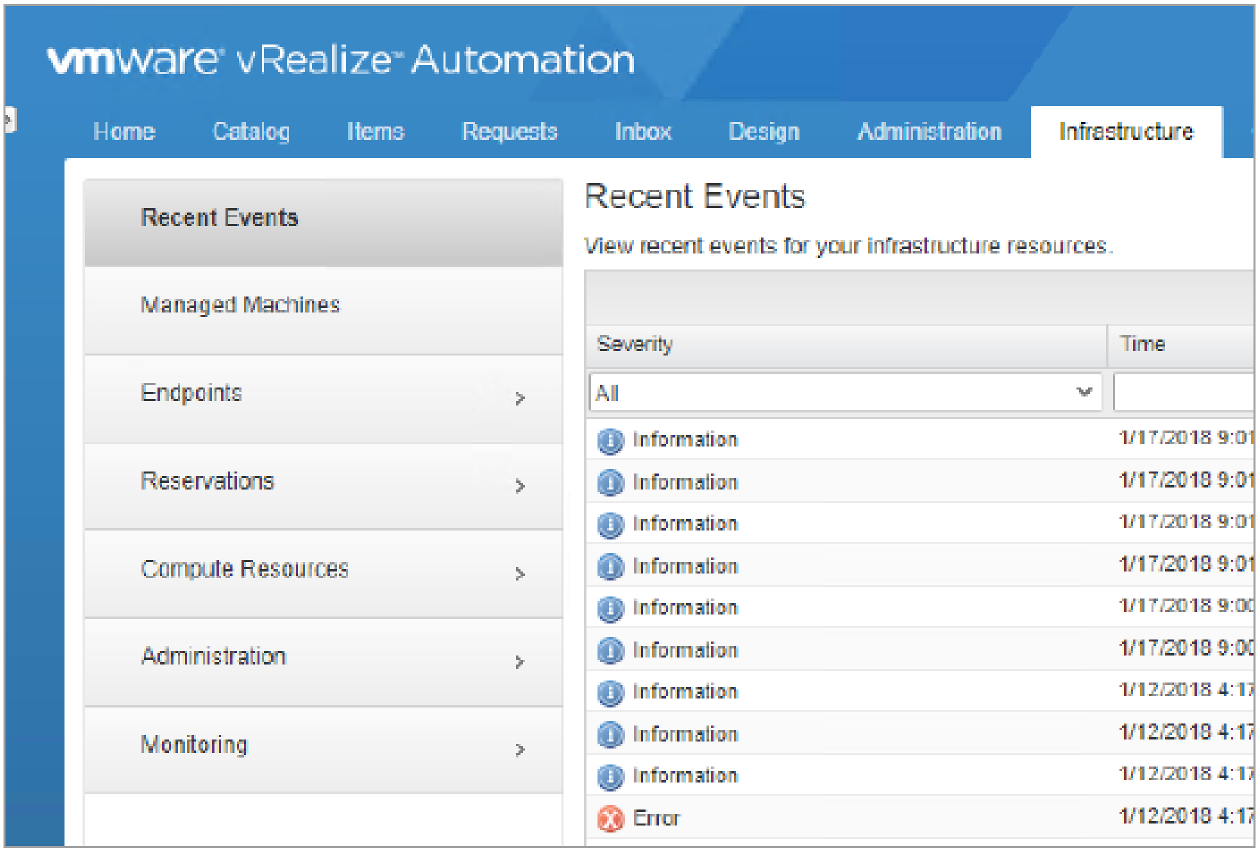
The Endpoint type is registered as shown below.



```
[2018-01-17 07:47:03.613] [I] Found existing host with url: https://vra-lab.lab.na/
[2018-01-17 07:47:03.629] [I] Found host to update: https://vra-lab.lab.na/
[2018-01-17 07:47:04.238] [I] VCAC host updated: DynamicWrapper (Instance) : [vCACCAFEHost]-[class com.vmware.o11n.plugin.vcac.model.VCACHo
[2018-01-17 07:47:04.627] [I] Created/updated endpoint category IPAM
[2018-01-17 07:47:04.836] [I] Creating endpoint type: SolarWinds
[2018-01-17 07:47:05.622] [I] Created/updated endpoint type SolarWinds
[2018-01-17 07:47:03.613] [I] Found existing host with url: https://vra-lab.lab.na/
[2018-01-17 07:47:03.629] [I] Found host to update: https://vra-lab.lab.na/
[2018-01-17 07:47:04.238] [I] VCAC host updated: DynamicWrapper (Instance) : [vCACCAFEHost]-[class com.vmware.o11n.plugin.vcac.model.VCACHo
[2018-01-17 07:47:04.627] [I] Created/updated endpoint category IPAM
[2018-01-17 07:47:04.836] [I] Creating endpoint type: SolarWinds
[2018-01-17 07:47:05.622] [I] Created/updated endpoint type SolarWinds
[2018-01-17 07:47:03.613] [I] Found existing host with url: https://vra-lab.lab.na/
[2018-01-17 07:47:03.629] [I] Found host to update: https://vra-lab.lab.na/
[2018-01-17 07:47:04.238] [I] VCAC host updated: DynamicWrapper (Instance) : [vCACCAFEHost]-[class com.vmware.o11n.plugin.vcac.model.VCACHo
[2018-01-17 07:47:04.627] [I] Created/updated endpoint category IPAM
[2018-01-17 07:47:04.836] [I] Creating endpoint type: SolarWinds
[2018-01-17 07:47:05.622] [I] Created/updated endpoint type SolarWinds
```

Register IPAM endpoint

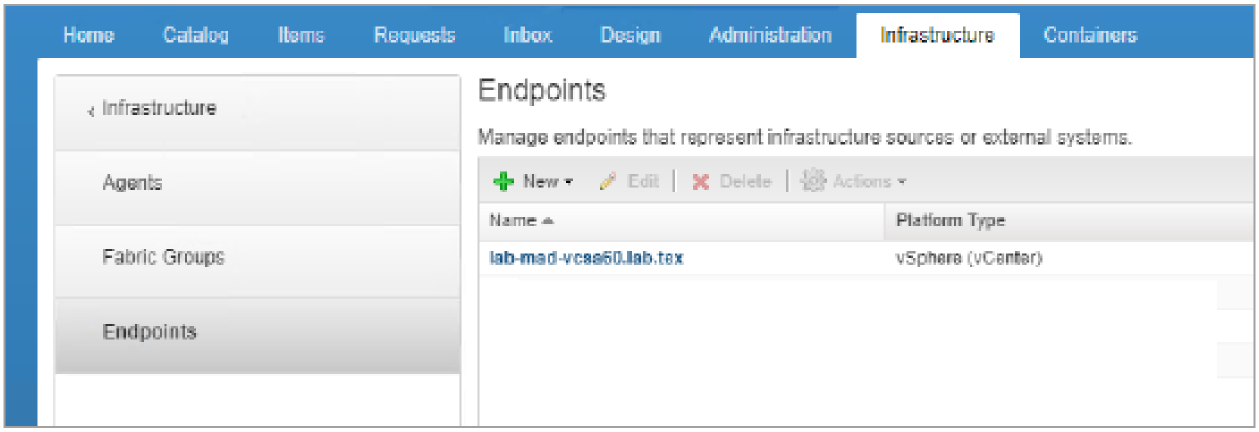
1. Log in into vRA.
2. Go to Infrastructure > Endpoints > Endpoints.



Recent Events

View recent events for your infrastructure resources.

Severity	Time
All	
Information	1/17/2018 9:01
Information	1/17/2018 9:01
Information	1/17/2018 9:01
Information	1/17/2018 9:01
Information	1/17/2018 9:00
Information	1/17/2018 9:00
Information	1/12/2018 4:17
Information	1/12/2018 4:17
Information	1/12/2018 4:17
Error	1/12/2018 4:17

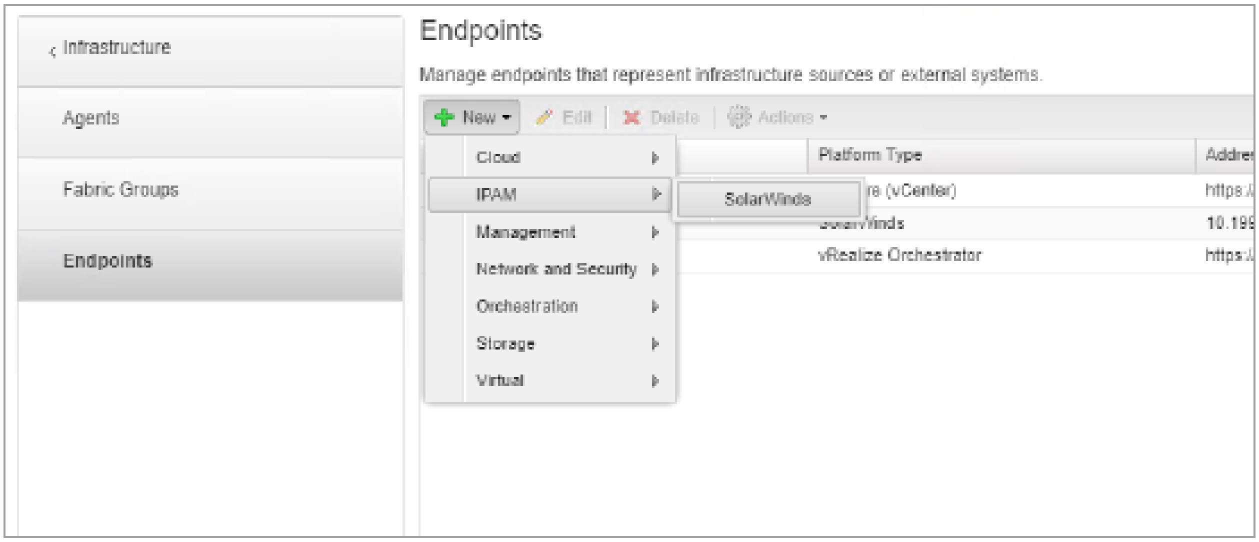


Endpoints

Manage endpoints that represent infrastructure sources or external systems.

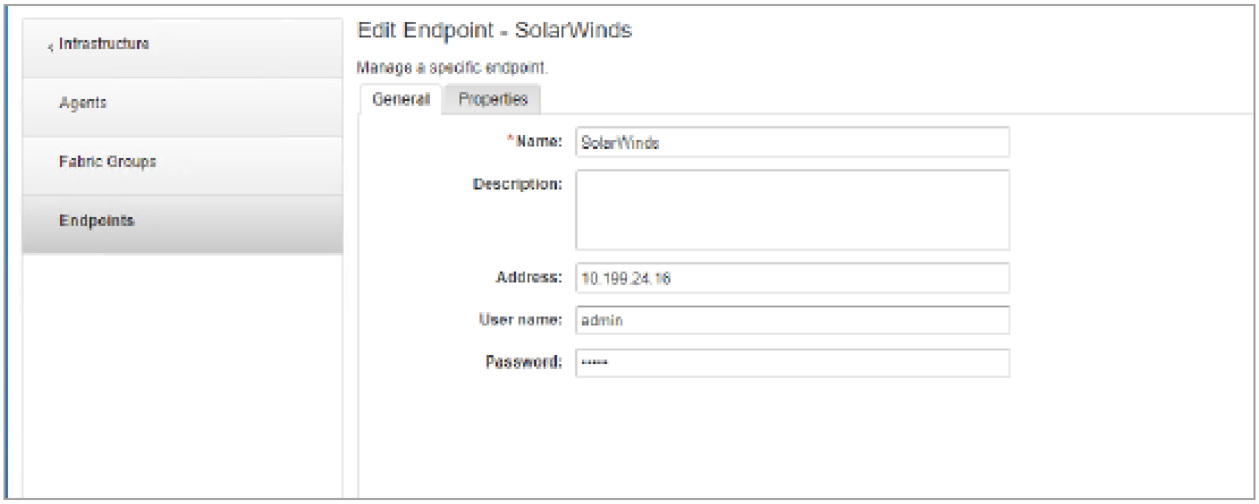
Name ▲	Platform Type
lab-mad-vcsa60.lab.tex	vSphere (vCenter)

3. Click New > IPAM > SolarWinds.



Manage endpoints that represent infrastructure sources or external systems.

4. Enter name, IP address (or hostname of installed IPAM), and SolarWinds credentials.



Edit Endpoint - SolarWinds

Manage a specific endpoint.

*Name: SolarWinds

Description:

Address: 10.199.24.16

User name: admin

Password: •••••

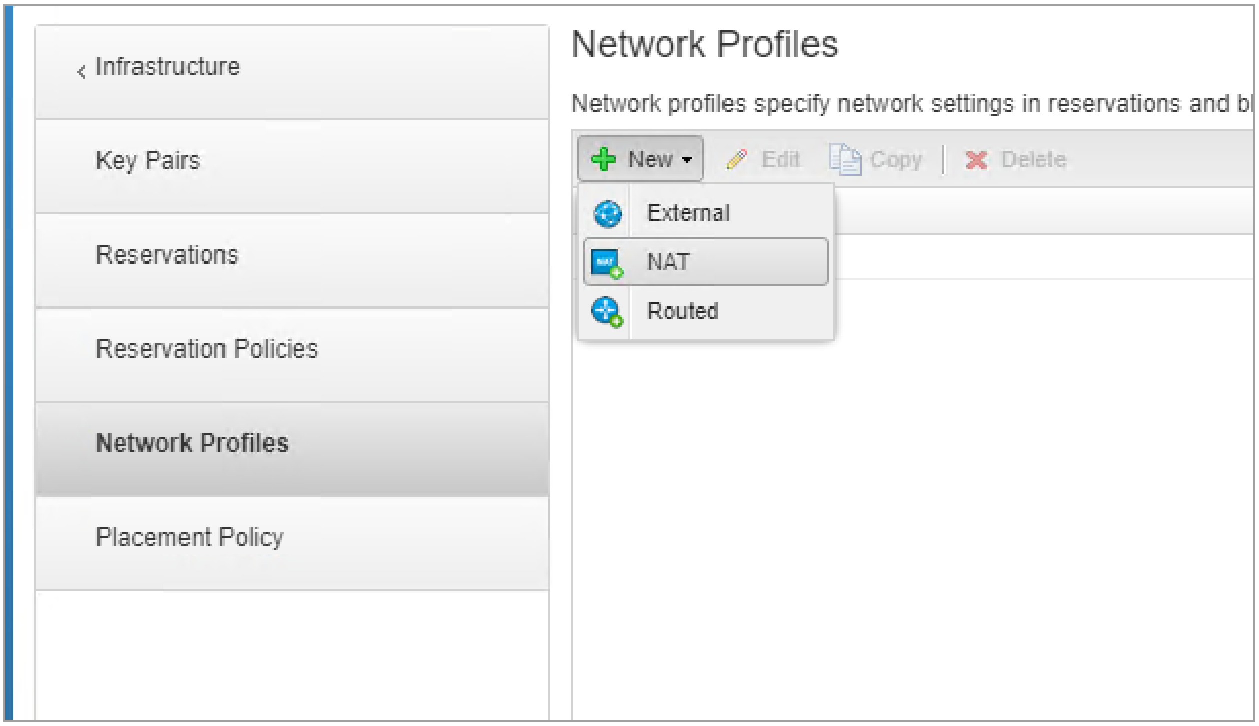
5. The following properties can be defined for endpoint connection on the Properties tab.

Property	Default value
connectionTimeout	30
operationTimeout	60
proxyHost	
proxyPort	0

6. Click OK.

Network profiles and reservations

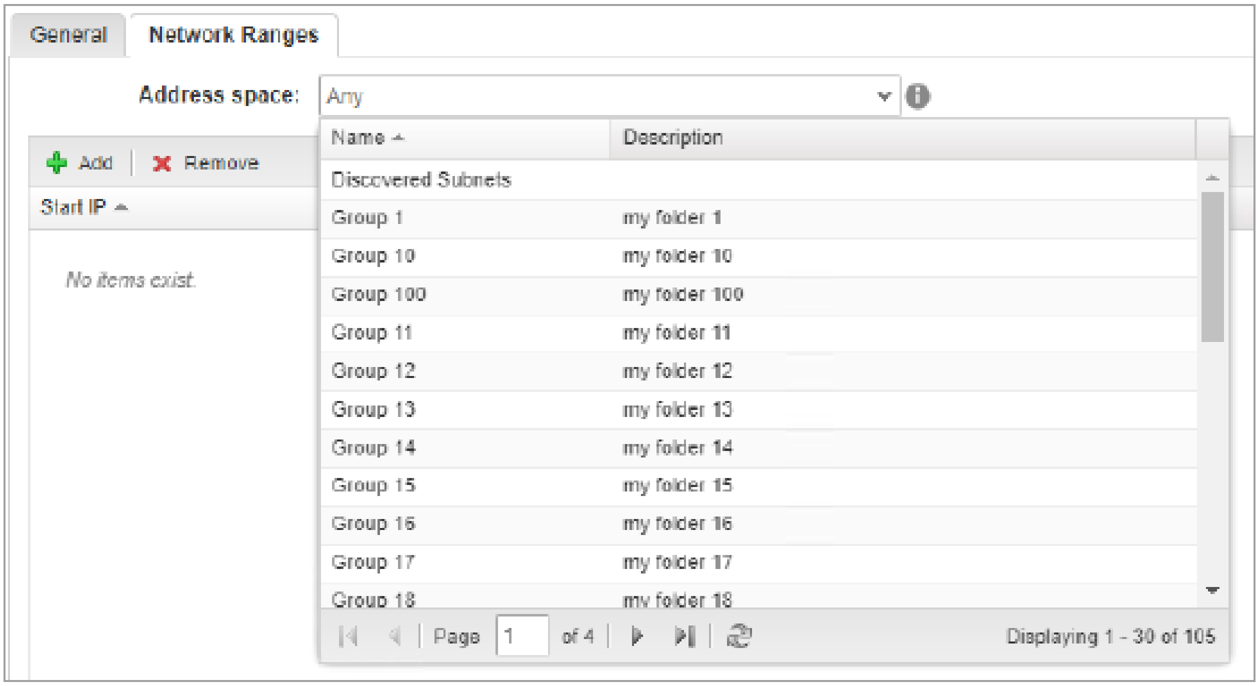
1. Go to Infrastructure > Reservations > Network Profiles, and then New > External to create anew network profile.



Network profiles specify network settings in reservations and bl

2. Define Name, and select SolarWinds in the IPAM endpoint combo box.

3. Open Network Ranges tab, and select Address Space,



Address space: Any

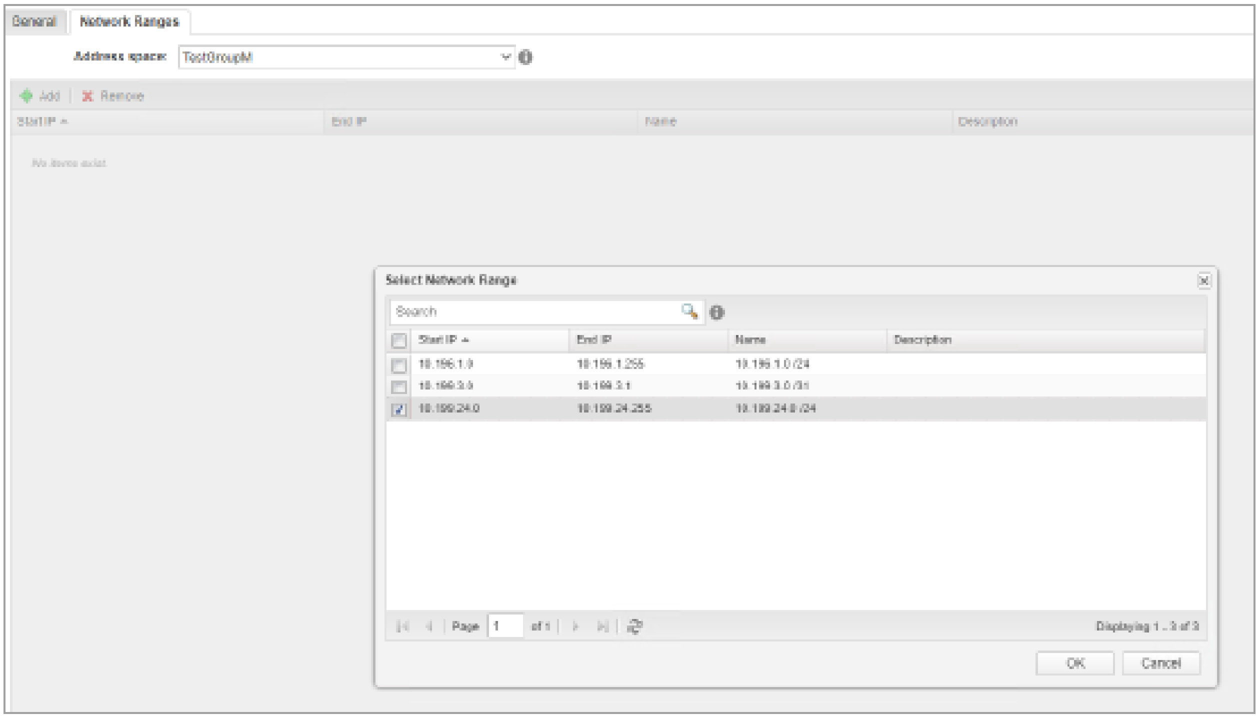
Name	Description
Discovered Subnets	
Group 1	my folder 1
Group 10	my folder 10
Group 100	my folder 100
Group 11	my folder 11
Group 12	my folder 12
Group 13	my folder 13
Group 14	my folder 14
Group 15	my folder 15
Group 16	my folder 16
Group 17	my folder 17
Group 18	my folder 18

No items exist.

Page 1 of 4

Displaying 1 - 30 of 105

4. Click Add, and click the search button to display available the subnets in IPAM group.



Address space: TestGroupM

	Start IP	End IP	Name	Description
□	10.196.1.0	10.196.1.255	10.196.1.0 /24	
□	10.199.3.0	10.199.3.1	10.199.3.0 /31	
☑	10.199.24.0	10.199.24.255	10.199.24.0 /24	

Page 1 of 1

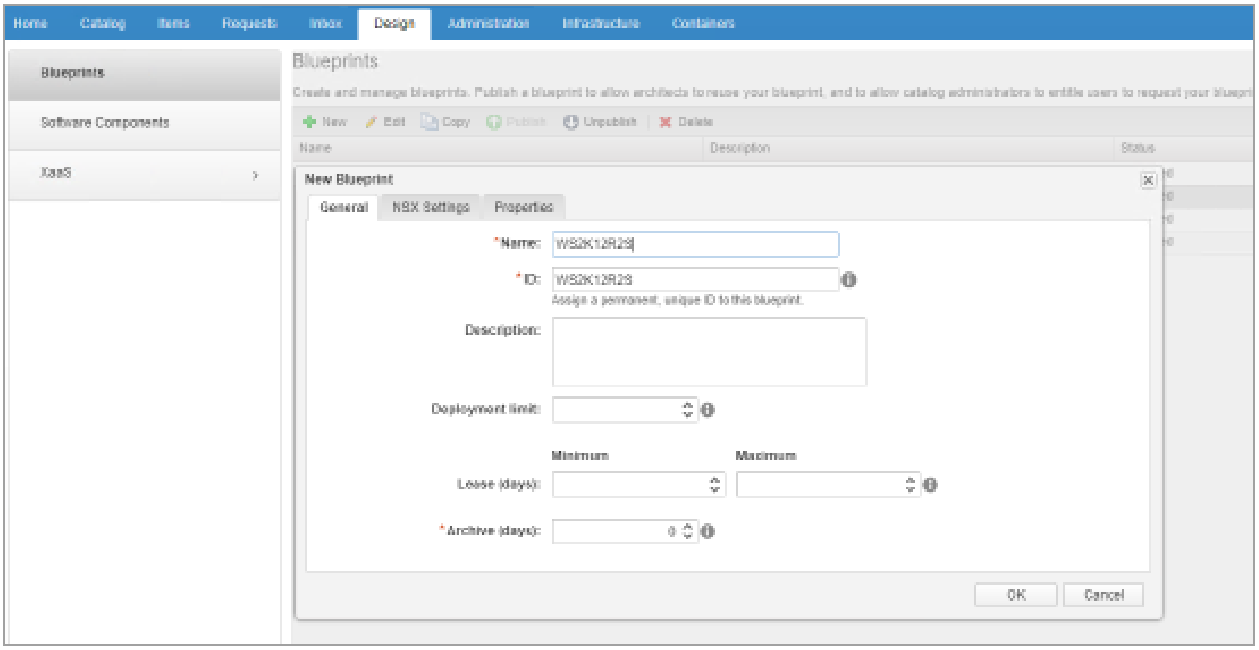
Displaying 1 - 3 of 3

5. Select the subnets,click OK, and click OK again to save the profile.

6. Go to Reservations, edit existing one and assign just created Network Profile for Network Adapter on Network tab.

Blueprint

1. Open Design > Blueprints and New.



Create and manage blueprints. Publish a blueprint to allow architects to reuse your blueprint, and to allow catalog administrators to entitle users to request your bluepri

*Name: WS2K12R2S

*ID: WS2K12R2S

Assign a permanent, unique ID to this blueprint.

Description:

Deployment limit:

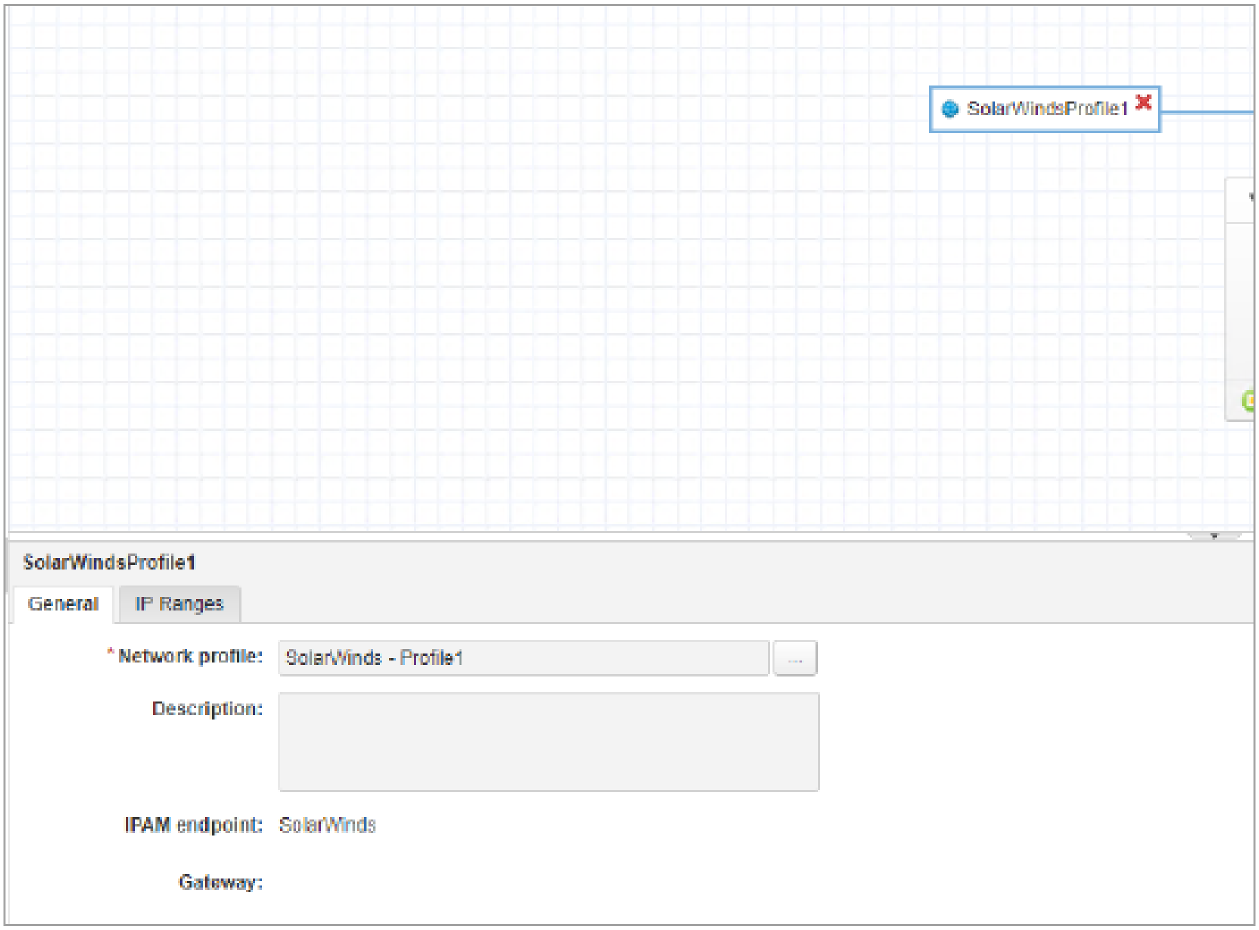
	Minimum	Maximum
Lease (days):		

*Archive (days): 0

2. Define Nameand the other.parameters, and click OK.

3. Add vSphere (vCenter) Machine and Existing Network components to Canvas.

4. Click Network component, and select Network Profile



SolarWindsProfile1

* Network profile: SolarWinds - Profile1

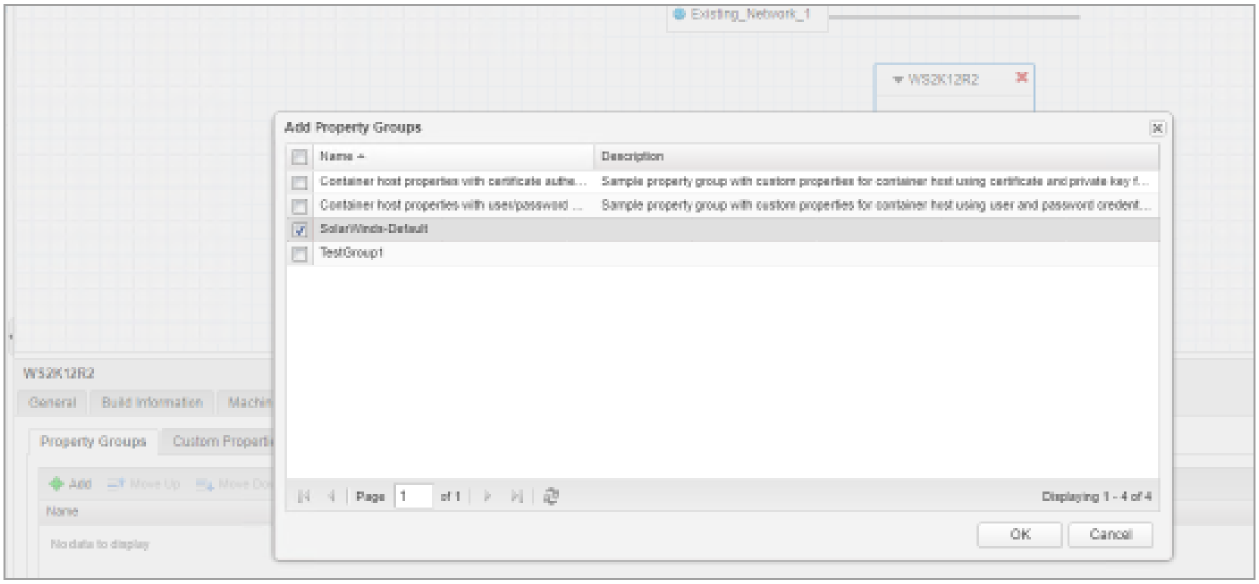
Description:

IPAM endpoint: SolarWinds

Gateway:

5. Click on the added machine component and:

   - On the Properties tab, add SolarWinds-Default properties.

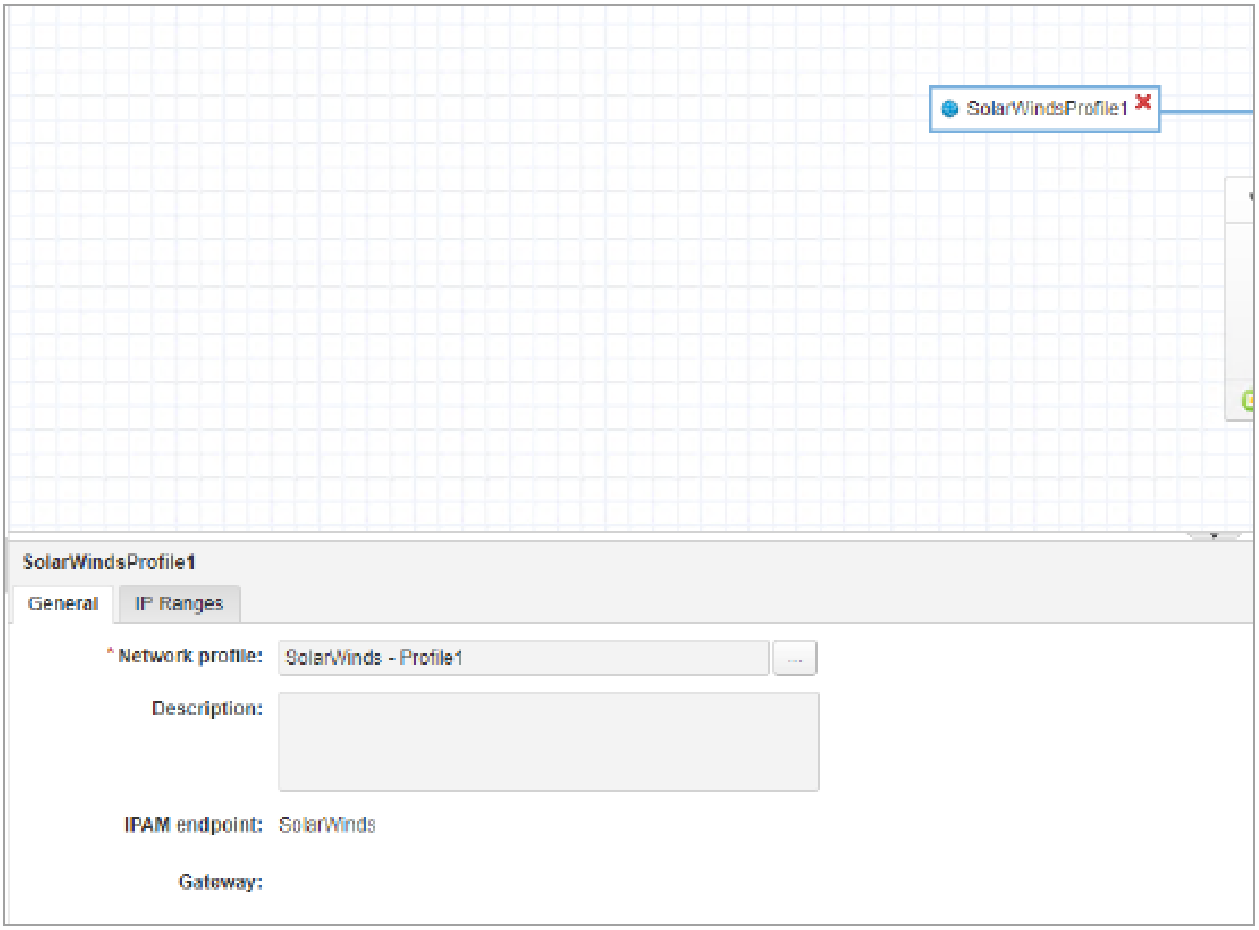


Add Property Groups

☐	Name ▲	Description
☐	Container host properties with certificate authe...	Sample property group with custom properties for container host using certificate and private key f...
☐	Container host properties with user/password ...	Sample property group with custom properties for container host using user and password credent...
☑	SolarWinds-Default	
☐	TestGroup1	

Displaying 1 - 4 of 4

   - On the Network tab, add network and select used profile,



* Network profile: SolarWinds - Profile1

Description:

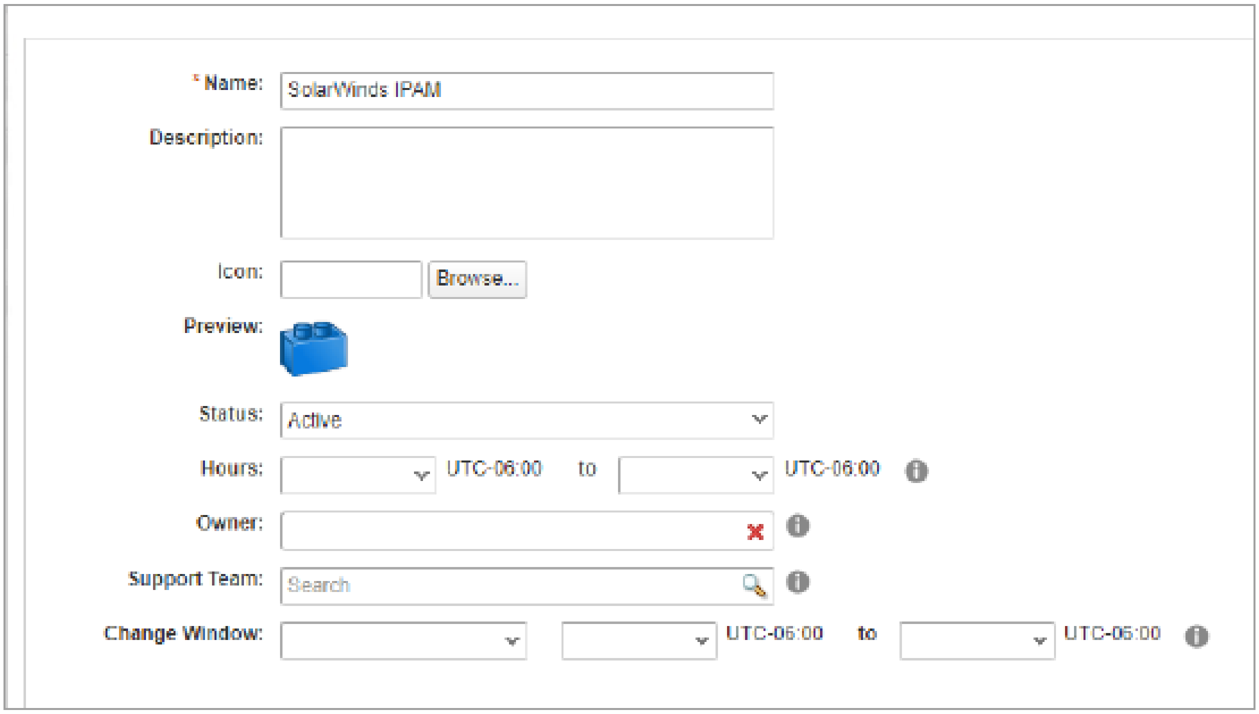
IPAM endpoint: SolarWinds

Gateway:

6. Click Save.

Publish the blueprint

1. Open Administration - Catalog Management - Services and click New.



* Name: SolarWinds IPAM

Description:

Icon: Browse...

Preview:

Status: Active

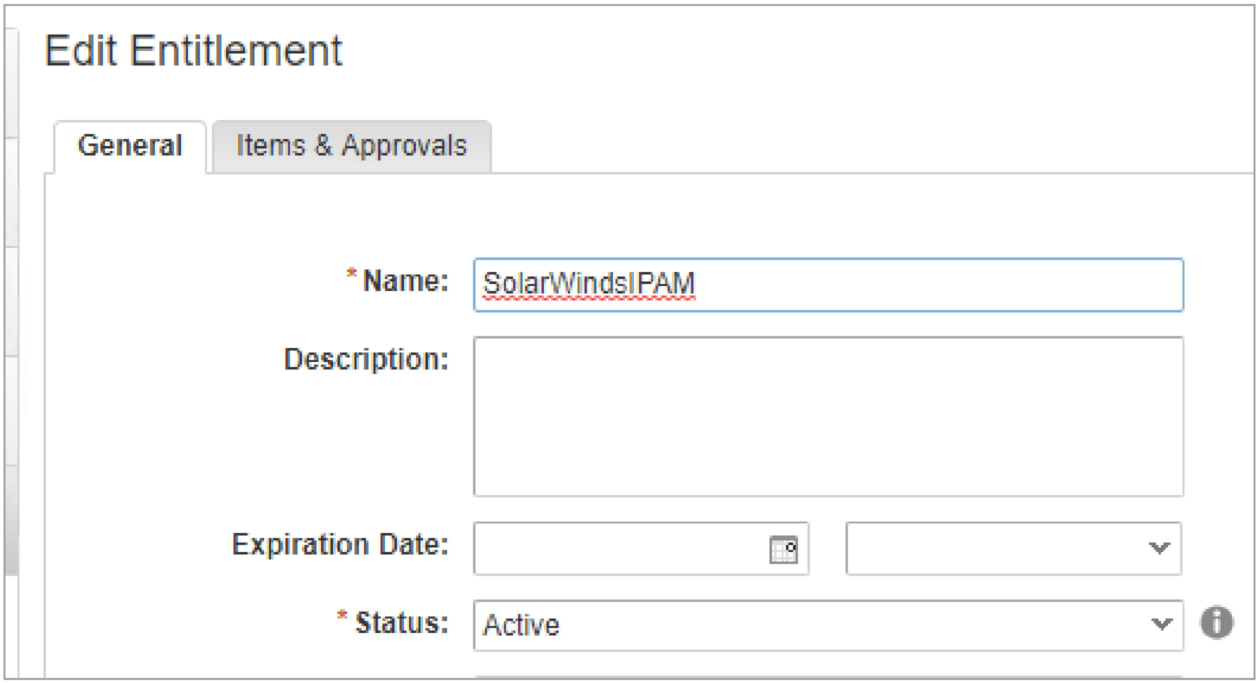
Hours: UTC-06:00 to UTC-06:00

Owner:

Support Team: Search

Change Window: UTC-06:00 to UTC-06:00

2. Enter details and click OK.
3. Open Administration - Catalog Management - Entitlements and click New.
4. Define name.



Edit Entitlement

General | Items & Approvals

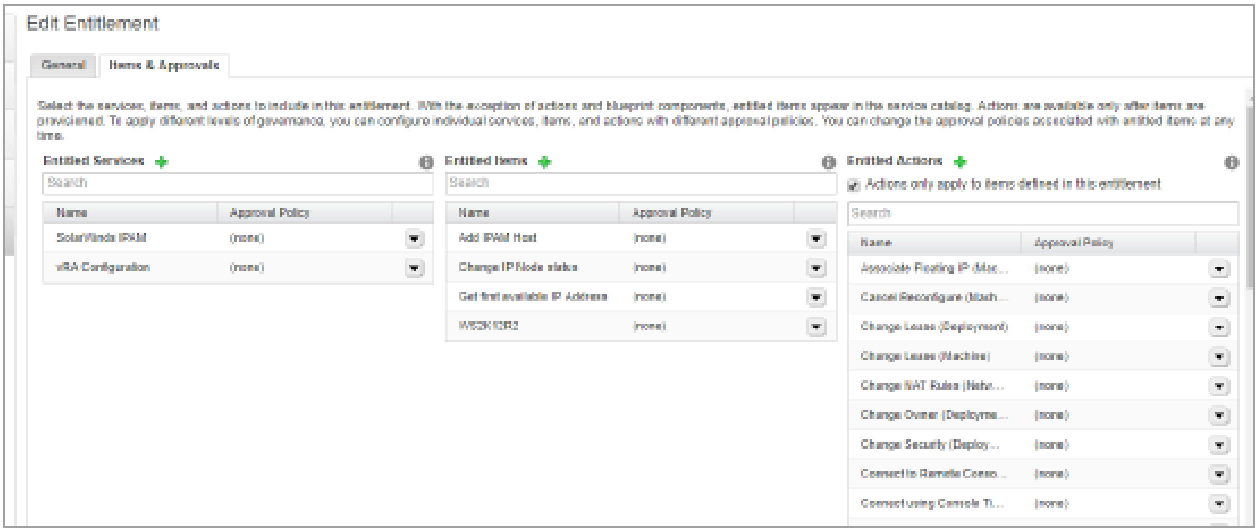
* Name: SolarWindsIPAM

Description:

Expiration Date:

* Status: Active

5. On the next tab add Services, and the blueprintyou created.



Edit Entitlement

Select the services, items, and actions to include in this entitlement. With the exception of actions and blueprint components, entitled items appear in the service catalog. Actions are available only after items are provisioned. To apply different levels of governance, you can configure individual services, items, and actions with different approval policies. You can change the approval policies associated with entitled items at any time.

Entitled Services

Name	Approval Policy
SolarWinds IPAM	(none)
vRA Configuration	(none)

Entitled Items

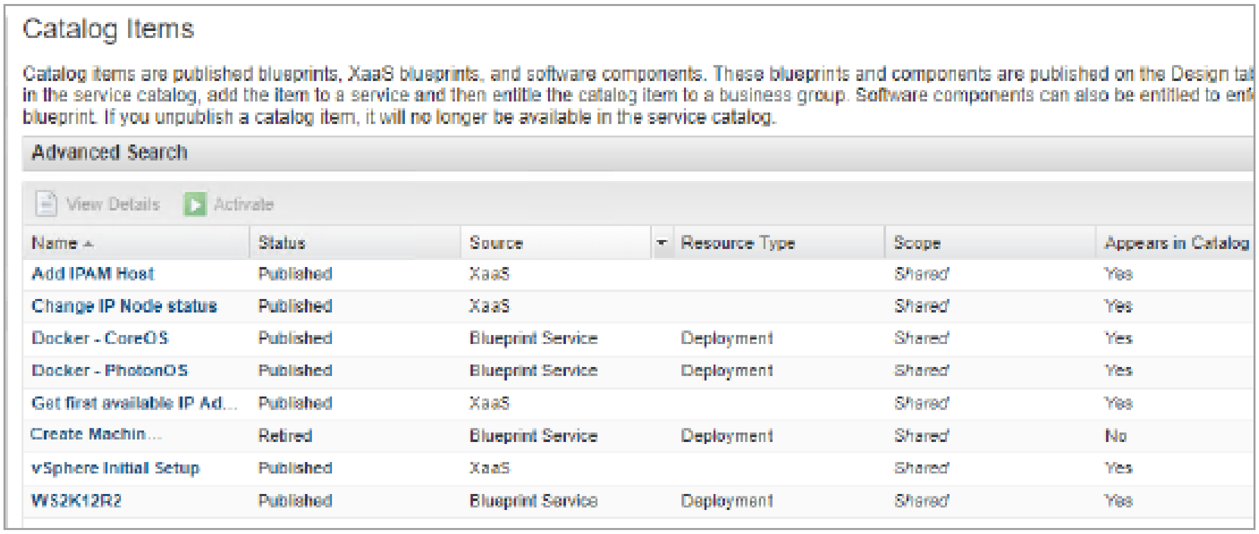
Name	Approval Policy
Add IPAM Host	(none)
Change IP Node status	(none)
Get first available IP Address	(none)
W52K12R2	(none)

Entitled Actions

☑ Actions only apply to items defined in this entitlement

Name	Approval Policy
Associate Floating IP (Mac...	(none)
Cancel Reconfigure (Mach...	(none)
Change Lease (Deployment)	(none)
Change Lease (Machine)	(none)
Change NAT Rules (Netw...	(none)
Change Owner (Deployme...	(none)
Change Security (Deploy...	(none)
Connect to Remote Conso...	(none)
Connect using Console Ti...	(none)

6. In the Catalog Items grid, select the blueprint you created, and activate it.



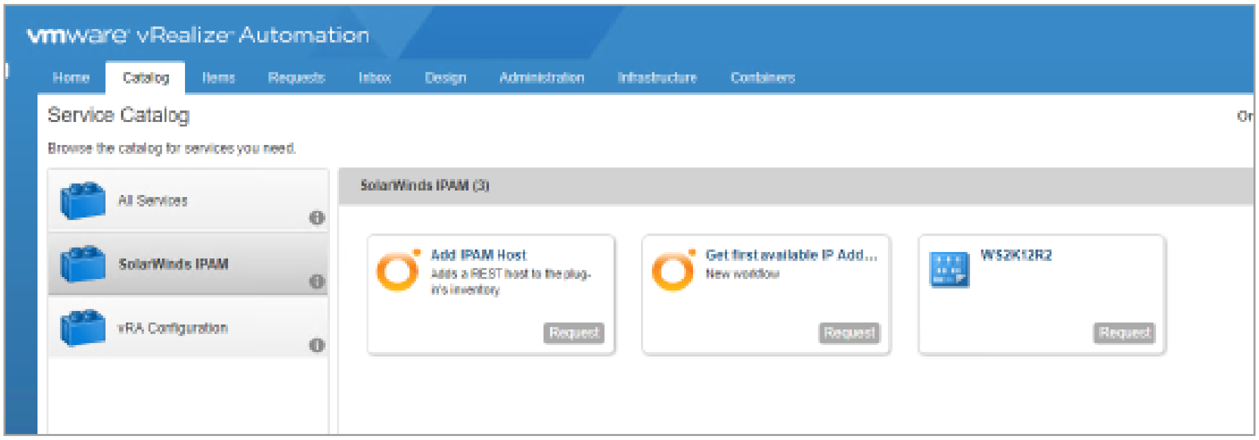
Catalog Items

Catalog items are published blueprints, XaaS blueprints, and software components. These blueprints and components are published on the Design tal in the service catalog, add the item to a service and then entitle the catalog item to a business group. Software components can also be entitled to enti blueprint. If you unpublish a catalog item, it will no longer be available in the service catalog.

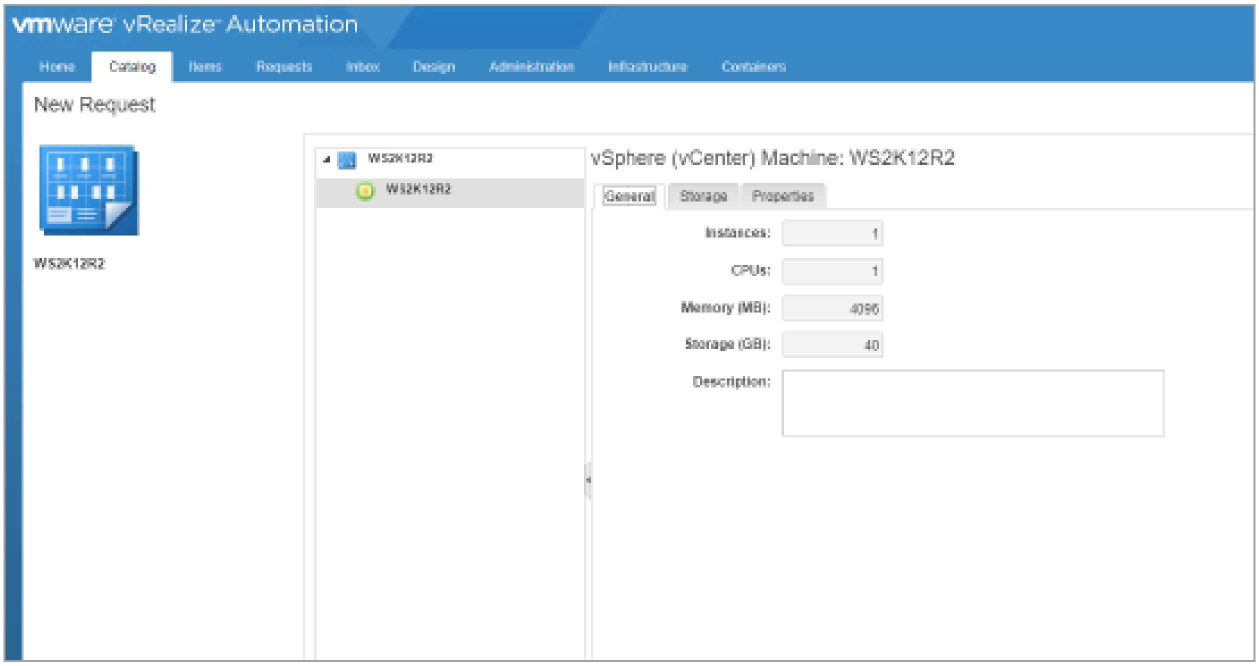
Name ▲	Status	Source	Resource Type	Scope	Appears in Catalog
Add IPAM Host	Published	XaaS		Shared	Yes
Change IP Node status	Published	XaaS		Shared	Yes
Docker - CoreOS	Published	Blueprint Service	Deployment	Shared	Yes
Docker - PhotonOS	Published	Blueprint Service	Deployment	Shared	Yes
Get first available IP Ad...	Published	XaaS		Shared	Yes
Create Machin...	Retired	Blueprint Service	Deployment	Shared	No
vSphere Initial Setup	Published	XaaS		Shared	Yes
W52K12R2	Published	Blueprint Service	Deployment	Shared	Yes

New machine

1. Click Catalog > SolarWinds IPAM, and then click Request on WS2K12R2 (the blueprint just created).



2. Select the machine to create.



vSphere (vCenter) Machine: WS2K12R2

Instances: 1

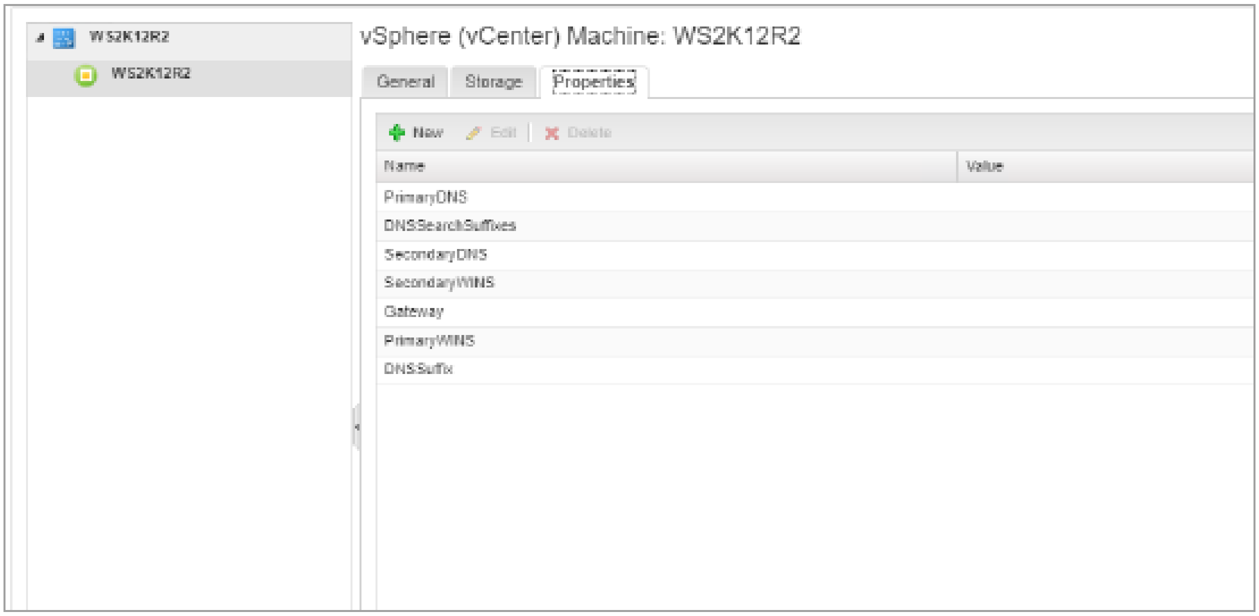
CPUs: 1

Memory (MB): 4096

Storage (GB): 40

Description:

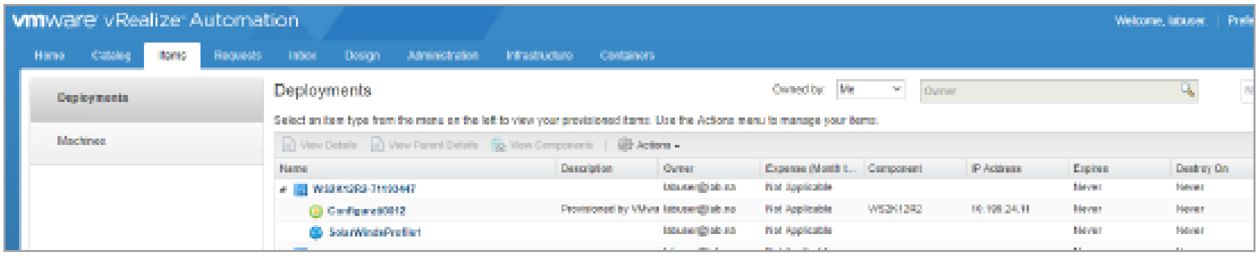
3. Define DNS properties if needed.



vSphere (vCenter) Machine: WS2K12R2

Name	Value
PrimaryDNS	
DNSSearchSuffixes	
SecondaryDNS	
SecondaryWINS	
Gateway	
PrimaryWINS	
DNSSuffix	

4. Click Submit. The VM will appear in the Items grid.



Deployments

Owned by: Me

Owner

Select an item type from the menu on the left to view your provisioned items. Use the Actions menu to manage your items.

Name	Description	Owner	Expires (Month t...	Component	IP Address	Expires	Destroy On
WS2K12R2-71110447		labuser@lab.xx	Not Applicable			Never	Never
Configure80812	Provisioned by VMwa	labuser@lab.xx	Not Applicable	WS2K12R2	10.198.24.11	Never	Never
SolarWindsProfile1		labuser@lab.xx	Not Applicable			Never	Never

Amazon Route 53 and Azure DNS monitoring

From version 4.7, IPAM enables you to monitor cloud DNS Zones and records from Amazon Route 53 and Azure DNS services. DNS zones from multiple cloud accounts for both services are displayed in a centralized view.

For more information on setting up cloud instances, please see Manage your cloud infrastructure in the SolarWinds section of this documentation for further information, or visit the Amazon and Azure support sites.

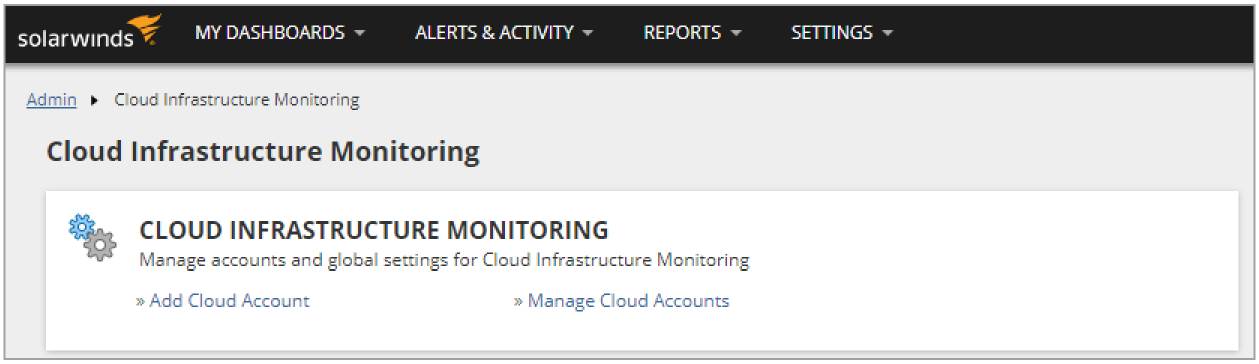
Add a Cloud account with DNS scanning in IPAM

1. Go to My Dashboards > Home > Cloud.

   The Cloud dashboard is displayed.

2. Click on the Cloud Infrastructure Monitoring Settings link in the upper right corner.

   The Cloud Infrastructure page is displayed.



Cloud Infrastructure Monitoring

CLOUD INFRASTRUCTURE MONITORING

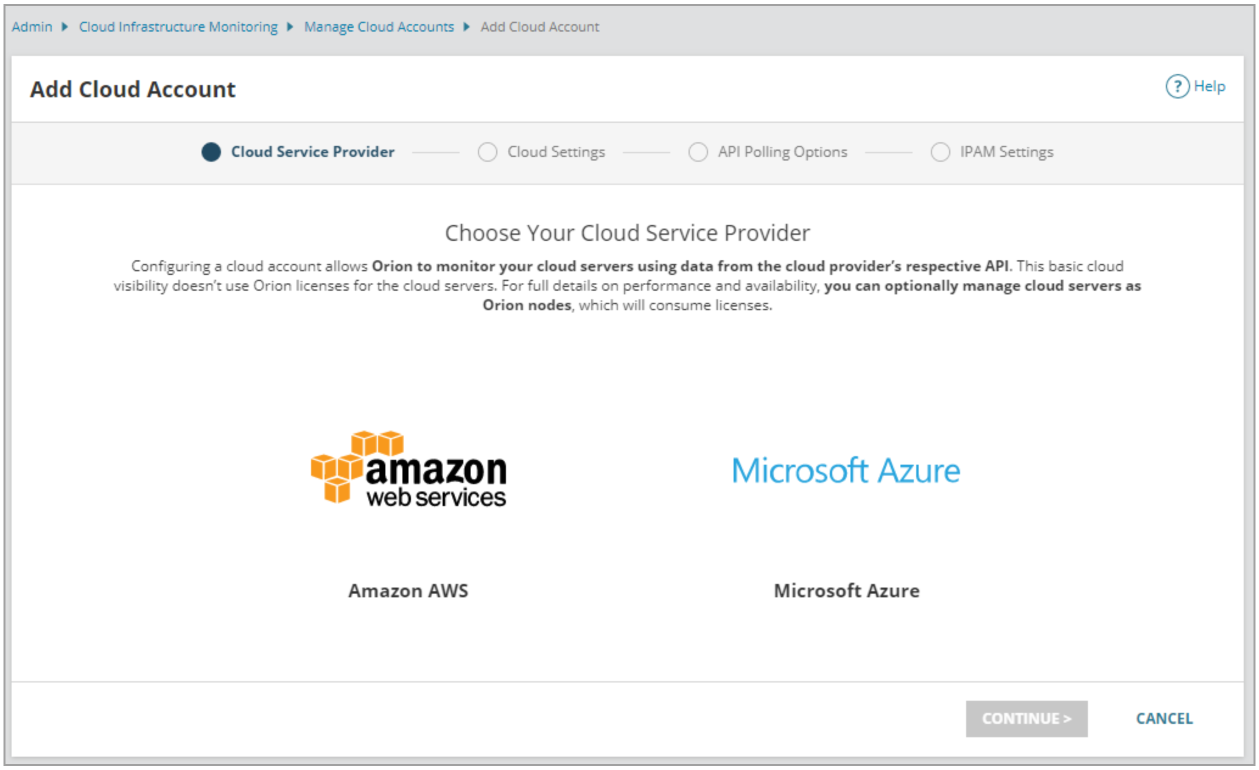
Manage accounts and global settings for Cloud Infrastructure Monitoring

» Add Cloud Account » Manage Cloud Accounts

3. Click Add Cloud Account.

   The Add Cloud Account page is displayed.

The stages shown, starting with Cloud Service Provider and ending with IPAM Settings, will depend on the SolarWinds products you have installed.



Admin ▸ Cloud Infrastructure Monitoring ▸ Manage Cloud Accounts ▸ Add Cloud Account

Add Cloud Account

● Cloud Service Provider — ○ Cloud Settings — ○ API Polling Options — ○ IPAM Settings

Choose Your Cloud Service Provider

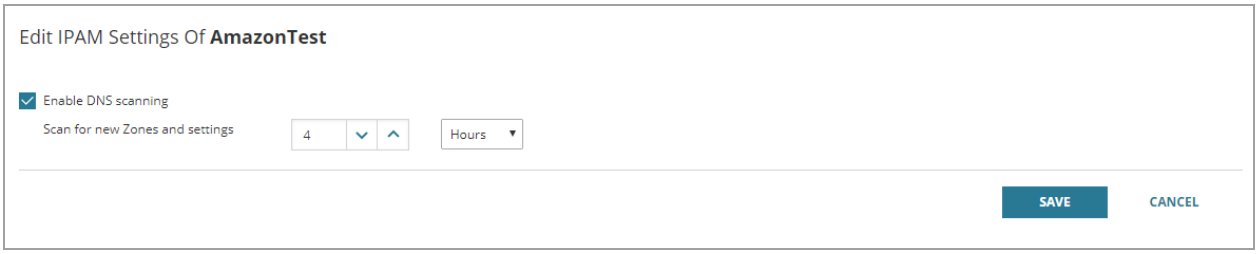
Configuring a cloud account allows **Orion to monitor your cloud servers using data from the cloud provider's respective API**. This basic cloud visibility doesn't use Orion licenses for the cloud servers. For full details on performance and availability, **you can optionally manage cloud servers as Orion nodes**, which will consume licenses.

4. Select the cloud service provider for which you want to add an account, and click Continue.

The Continue button will change to Monitor AWS or Monitor Azure depending on your selection.

5. Enter the Cloud account display name.
6. Enter the Credentials for the account. For information finding these for both AWS and Azure accounts, see [Find cloud account credentials](#).
7. Complete the other stages as relevant to your account.

   See [Manage your cloud infrastructure for more information](#).



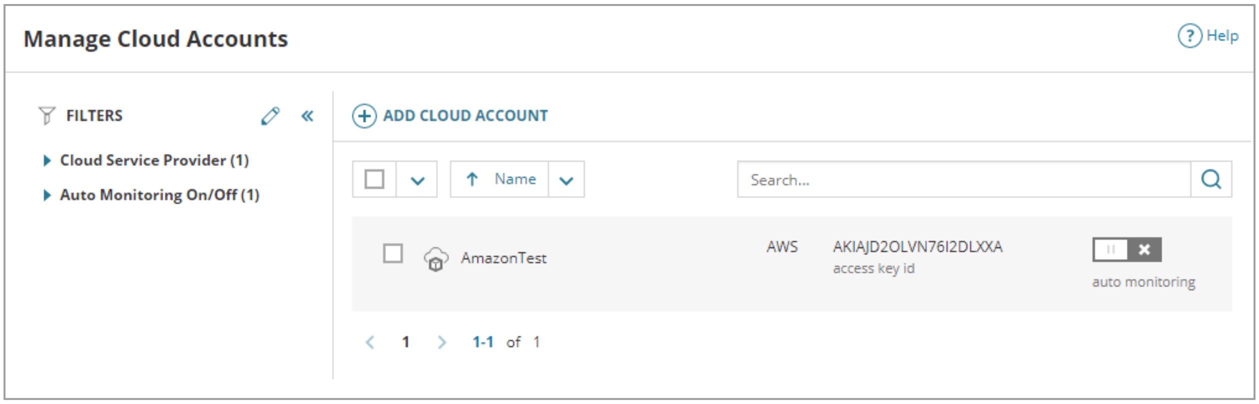
Edit IPAM Settings Of **AmazonTest**

☑ Enable DNS scanning

Scan for new Zones and settings: 4 Hours

8. At the IPAM Settings stage, select Enable DNS scanning, specify the scan time interval, and click Finish.

   The Manage Cloud Accounts page is displayed, showing the account you added, showing the access key ID.



Manage Cloud Accounts

FILTERS

- Cloud Service Provider (1)
- Auto Monitoring On/Off (1)

□ AmazonTest	AWS	AKIAJD2OLVN76I2DLXXA access key id	auto monitoring

1 1-1 of 1

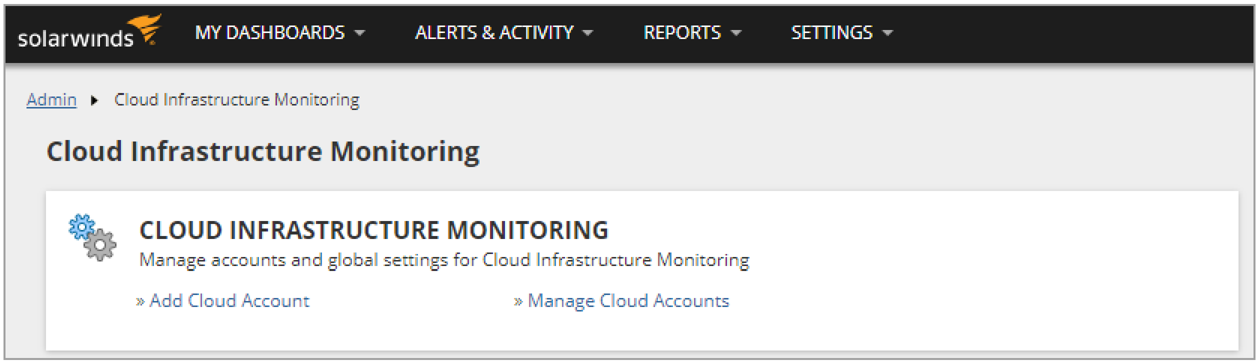
Manage IPAM settings for a cloud account

1. Go to My Dashboards > Cloud.

   The Cloud dashboard is displayed.

2. Click on the Cloud Infrastructure Monitoring Settings link in the upper right corner.

   The Cloud Infrastructure page is displayed.



Admin ▸ Cloud Infrastructure Monitoring

Cloud Infrastructure Monitoring

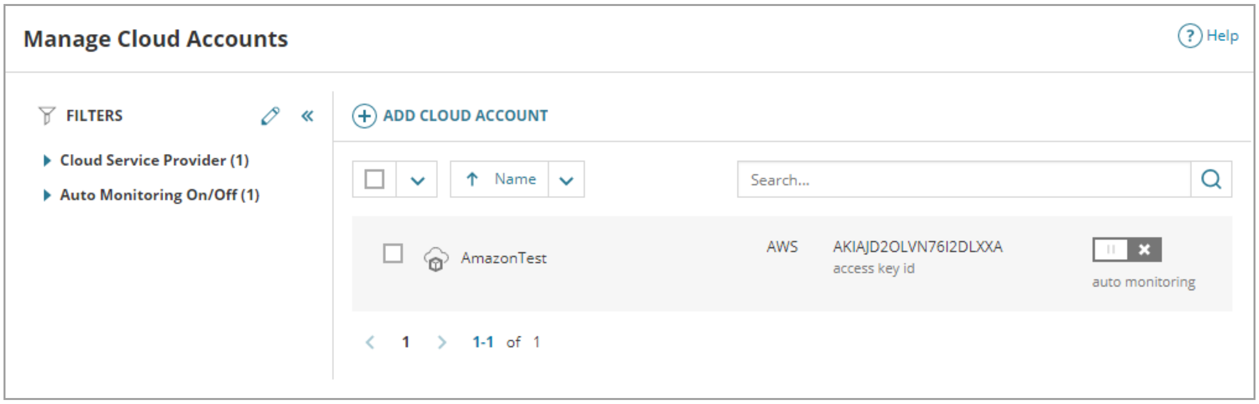
CLOUD INFRASTRUCTURE MONITORING

Manage accounts and global settings for Cloud Infrastructure Monitoring

» Add Cloud Account » Manage Cloud Accounts

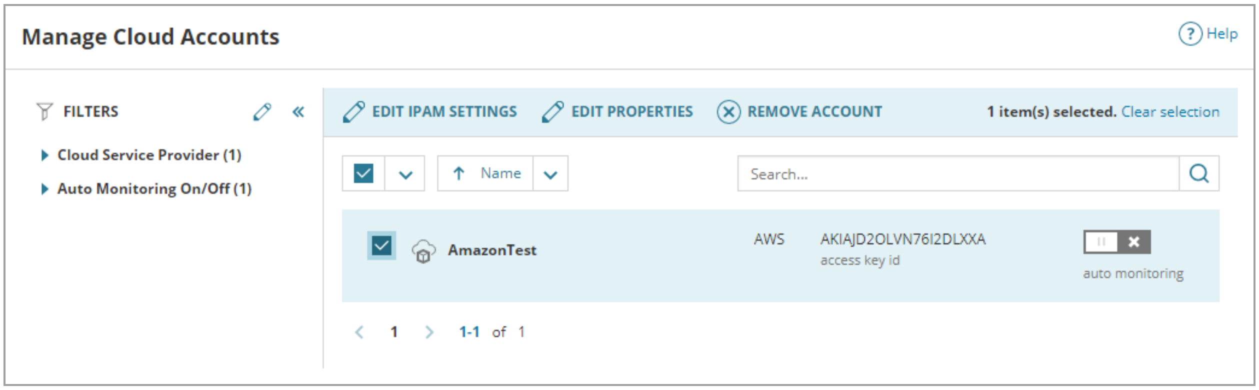
3. Click Manage Cloud Accounts.

   The Manage Cloud Accounts page is displayed. Here you can enable or disable auto-monitoring.



4. Select the required account or accounts.

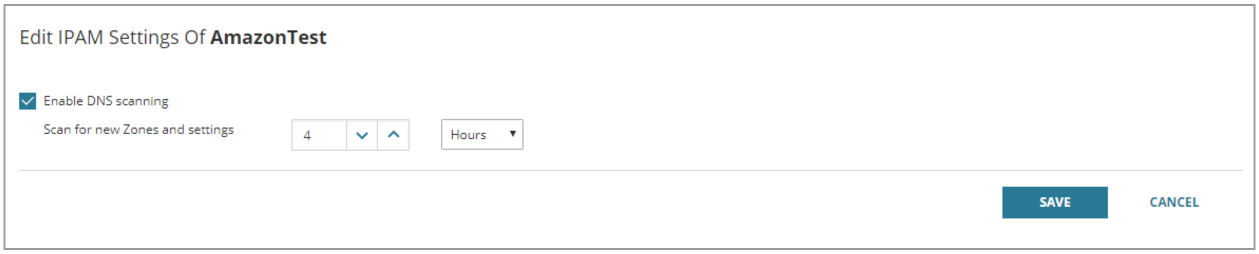
   When you select accounts, a number of options are displayed.



5. Click Edit IPAM Settings.

   Here you can:

   - Enable/disable DNS scanning
   - Change the scanning interval


Edit IPAM Settings Of **AmazonTest**

☑ Enable DNS scanning

Scan for new Zones and settings 4 Hours

Add new Cloud DNS zones to IPAM

You cannot add new Cloud DNS zones/records to a Cloud account from within IPAM. You need to add these to the account via the Azure or AWS web site. See the documentation for the appropriate service for further information:

- Amazon Route 53 (external link)
- Microsoft Azure (external link)

Monitoring Cloud DNS zones and records in IPAM

From the release of IPAM 4.7, you can view your Amazon Route 53 and Azure DNS zones and corresponding records.

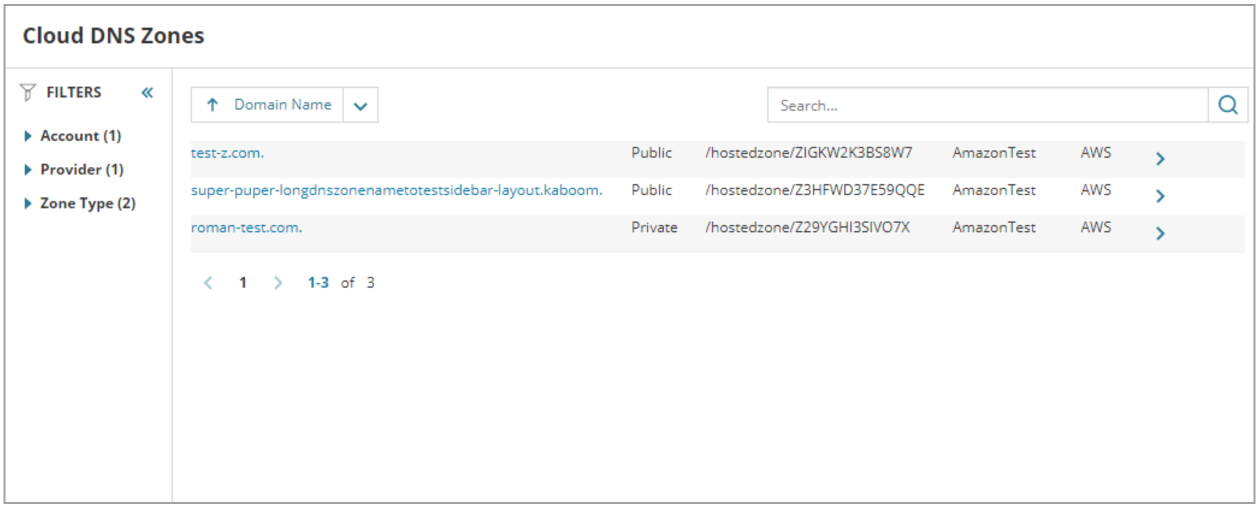
1. Go to My Dashboards > Cloud.

   The Cloud dashboard is displayed.

2. Click on the Cloud DNS Zones icon in the left column.

   > ⓘ If the icon is not displayed, check that IPAM 4.7 or higher is installed.

   The Cloud DNS Zones page is displayed.



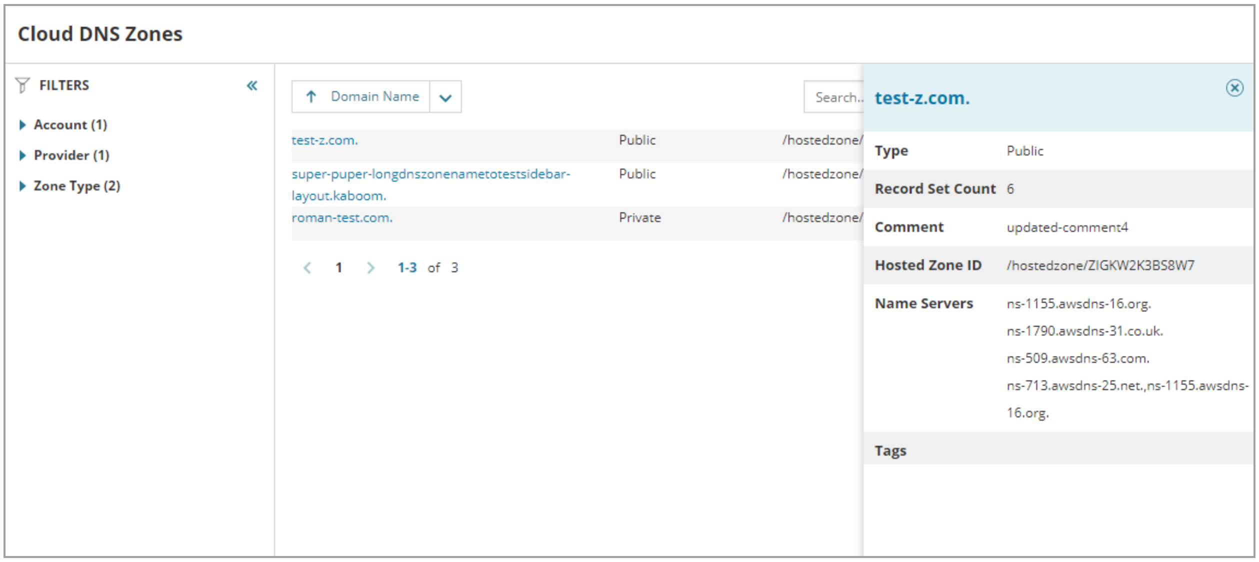
Cloud DNS Zones

test-z.com.	Public	/hostedzone/ZIGKW2K3BS8W7	AmazonTest	AWS
super-puper-longdnszonenametotestsidebar-layout.kaboom.	Public	/hostedzone/Z3HFWD37E59QQE	AmazonTest	AWS
roman-test.com.	Private	/hostedzone/Z29YGHI3SIVO7X	AmazonTest	AWS

3. Here you can:

   - Filter the list of DNS Zones being monitored by account, provider or zone type (public or private).
   - List zones by domain name, type, account or provider.

- See further information by clicking the blue chevron



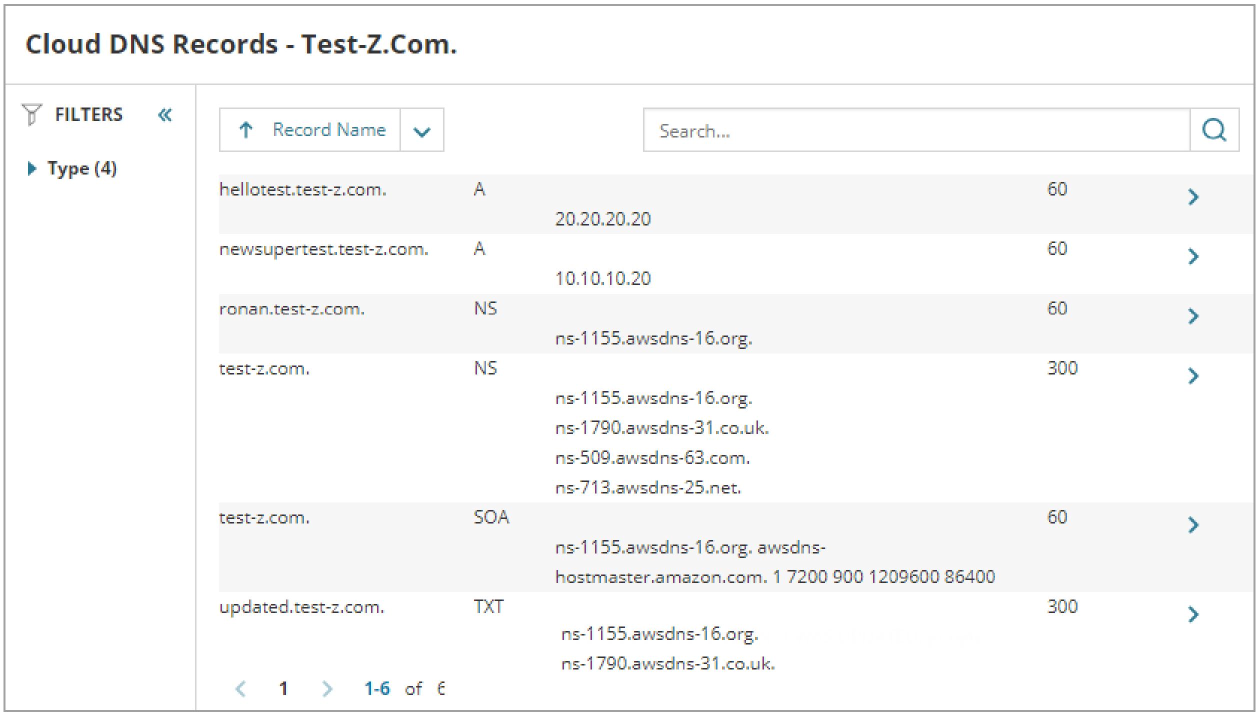
Cloud DNS Zones

test-z.com.	Public	/hostedzone/
super-puper-longdnszonenametotestsidebar-layout.kaboom.	Public	/hostedzone/
roman-test.com.	Private	/hostedzone/

test-z.com.

Type	Public
Record Set Count	6
Comment	updated-comment4
Hosted Zone ID	/hostedzone/ZIGKW2K3BS8W7
Name Servers	ns-1155.awsdns-16.org. ns-1790.awsdns-31.co.uk. ns-509.awsdns-63.com. ns-713.awsdns-25.net.,ns-1155.awsdns-16.org.
Tags	

4. Click a domain name to display the Cloud DNS Records page for that domain.



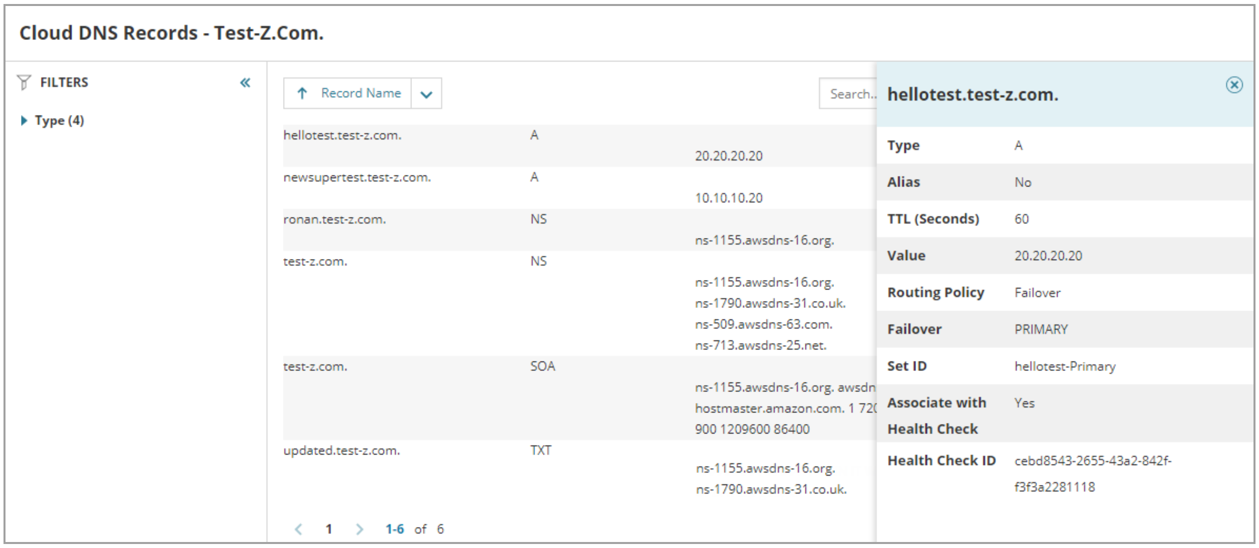
Cloud DNS Records - Test-Z.Com.

hellotest.test-z.com.	A	20.20.20.20	60
newsupertest.test-z.com.	A	10.10.10.20	60
ronan.test-z.com.	NS	ns-1155.awsdns-16.org.	60
test-z.com.	NS	ns-1155.awsdns-16.org. ns-1790.awsdns-31.co.uk. ns-509.awsdns-63.com. ns-713.awsdns-25.net.	300
test-z.com.	SOA	ns-1155.awsdns-16.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400	60
updated.test-z.com.	TXT	ns-1155.awsdns-16.org. ns-1790.awsdns-31.co.uk.	300

5. Here you can:

- Filter the list of DNS Records being monitored by type.
- List records by record name, type, value or TTL.

- View further information by clicking the blue chevron.



Cloud DNS Records - Test-Z.Com.

hellotest.test-z.com.	A	20.20.20.20
newsupertest.test-z.com.	A	10.10.10.20
ronan.test-z.com.	NS	ns-1155.awsdns-16.org.
test-z.com.	NS	ns-1155.awsdns-16.org. ns-1790.awsdns-31.co.uk. ns-509.awsdns-63.com. ns-713.awsdns-25.net.
test-z.com.	SOA	ns-1155.awsdns-16.org. awsdn hostmaster.amazon.com. 1 720 900 1209600 86400
updated.test-z.com.	TXT	ns-1155.awsdns-16.org. ns-1790.awsdns-31.co.uk.

hellotest.test-z.com.

Type	A
Alias	No
TTL (Seconds)	60
Value	20.20.20.20
Routing Policy	Failover
Failover	PRIMARY
Set ID	hellotest-Primary
Associate with Health Check	Yes
Health Check ID	cebd8543-2655-43a2-842f-f3f3a2281118

Monitor cloud instances and VMs

Cloud service platforms provide on-demand computing resources to third-party organizations over the Internet. As organizations migrate systems to the cloud to distribute workloads, deliver applications, and expand resources for growing databases, infrastructure can become difficult to map in sprawling environments, leading to lost resources or hidden instances.

To support hybrid environments, the IP Address Manager can retrieve data from the Amazon Web Services (AWS) and Microsoft Azure cloud service platforms to track availability, performance, applications, and more for instances and VMs. Examples of data gathered include status, storage capacity, memory usage, and IP addresses.

Using the Cloud Infrastructure Monitoring feature with IP Address Manager products such as SolarWinds SAM and VMAN provides several benefits, including the ability to:

- Manage hybrid environment metrics and status through a single console. Displaying on-premises, virtual, and cloud systems together helps you compare performance, locate bottlenecks, and better plan capacity and resource allocation.
- Track end user and business context for performance by using SolarWinds SAM to gather extended metrics that provide visibility into cloud and on-premises systems.
- Dynamically monitor cloud instances and VMs to better handle resource churn during provisioning. Instances and VMs can be removed as needed to support expanding environments or performance peaks.
- Determine usage trends and troubleshoot issues. Captured metrics over time provide historical references to track trends for resource consumption (such as CPU spikes and lulls) and help determine when those trends become issues.

- Use cloud monitoring data, SolarWinds alerts, and the Performance Analysis dashboard (PerfStack) to review historical performance and pinpoint when significant usage changes began to trigger issues.

To enhance cloud monitoring, configure cloud instances/VMs as managed nodes in the IP Address Manager so that you can:

- Poll specific metrics beyond the basic metrics gathered by cloud service APIs, including OS, memory, and other detailed metrics retrieved by SAM application monitors.
- Use SAM application monitors and templates to poll applications deployed in the cloud.
- Display cloud instance/VM details in AppStack for quick troubleshooting across your environment.
- Develop and deploy custom script monitors for PowerShell, Nagios, Linux/UNIX, and Windows.
- Assign Custom Properties to nodes.

To learn more, see Manage a cloud instance/VM as an IP Address Manager node.

Cloud monitoring recommendations

For optimal performance, SolarWinds recommends the following limits for cloud monitoring:

- Up to 10 cloud service accounts
- Up to 1,000 instances/VMs to monitor
- Up to 1,000 volumes to monitor
- Up to 1,000 instances/VMs managed as nodes
- Up to 1,000 SolarWinds agents deployed on managed nodes

Before exceeding recommended limits, consider the impact on polling load, costs incurred due to API request overages, and the possible need to expand hardware, CPU resources, memory, etc.

Cloud monitoring requirements

Several IP Address Manager products support the Cloud Infrastructure Monitoring feature, including SolarWinds SAM and VMAN.

Functionality	Requirements
Monitor AWS cloud metrics	An AWS account configured for cloud monitoring. You will need the following credentials to add an account to the IP Address Manager or deploy SolarWinds agents to instances: • Access Key ID • Secret Access Key

Functionality	Requirements
Monitor Azure cloud metrics	An Azure account configured for cloud monitoring. You will need the following credentials to add an account to the IP Address Manager or deploy SolarWinds agents to VMs: • Subscription ID • Tenant/Directory ID • Client/Application ID • Application Secret Key ⓘ The IP Address Manager supports VMs deployed via the Azure Resource Manager but not VMs created using a classic deployment model.

ⓘ The SolarWinds server must be configured to communicate with public services to collect data from cloud service APIs. Use the default setting — public — in community strings for polled devices to allow read access.

After you configure a cloud account and add an initial cloud account to the IP Address Manager, cloud services start polling for metrics, as displayed on the Cloud Summary page in the SolarWinds Platform Web Console. See Explore cloud instances and VMs on the Cloud Summary page.

Cloud metrics vs. OS metrics

Cloud services APIs, such as the Amazon CloudWatch API and Azure Rest API, capture basic metric data for instances/VMs and volumes so you can allocate resources as needed, such as partial CPU processing and disk space across multiple instances/VMs. These resources can change through direct interactions and automation. For example, when the Amazon EC2 web service reports data to the IP Address Manager, it calculates the percentage of assigned resources shared between instances.

Cloud metrics differ with OS metrics due to the fluid nature of cloud computing. OS metrics directly capture values from the core system, not the assigned amounts. This data does not calculate shared resources or other users attached to the instances and volumes. This data directly displays the actual usage at a polled point in time.

Both cloud metrics and OS metrics provide insight into potential and actual issues with performance and resources. Metrics report vastly different information to the cloud and OS based on allocated resources and metric calculations.

CPU steal is an example of cloud vs. OS metrics. When CPU usage and metrics spike in a cloud environment, multiple processes and instances/VMs in the cloud may access the CPU as multiple owners. Typically, OS metric spikes tend to look like noisy neighbors. The cloud metric data better represents the data as shared resources usage across multiple owners with metrics broken down by owner.

To better define resource usage and alerts, SAM and integrated VMAN display cloud instance/VM metrics throughout all cloud resources in SolarWinds Platform Web Console views, resources, hover-over data, and reports. Cloud metrics, including calculated health status, CPU load, and IOPS data, are used to apply global cloud thresholds that trigger alerts and status changes. For a list of cloud metrics gathered by cloud service APIs, see the table included in the Edit global thresholds for cloud monitoring topic.

For instances and VMs managed as nodes, the IP Address Manager pulls specific OS data for memory and provides additional data through SolarWinds agent, WMI, and SNMP polling methods.

Use the SWIS API to perform IPAM operations

You can use Windows PowerShell and the SolarWinds SDK to manage IP addresses in IPAM. The IPAM-specific API fields are documented on the IPAM API wiki page in the SolarWinds SDK.

> ⓘ Currently IPAM API does not support parallel execution of tasks.

Supported operations:

- Get the first available IP address for a specified subnet
- Change IP node status
- Start, finish, and cancel an IP address reservation
- Create a new subnet
- Add a DNS 'A' record for an IP address
- Change a DNS 'A' record for an IP address
- Remove a DNS 'A' record for an IP address
- Add an 'A' record with an associated PTR for a zone
- Add PTR to a DNS 'A' record
- Create an IP address reservation on a DHCP server
- Remove an IP address reservation from a DHCP server
- Get an 'A' recorde and PTR records for a DNS zone
- Create a custom property
- Update a custom property
- Reorder a custom property
- Delete a custom property
- CRUD operations for subnets
- CRUD operations for IP addresses

Pre-requisites

- Verify that at least PowerShell 4.0 is installed:
  - Open PowerShell and enter $PSVersionTable.PSVersion to determine the PowerShell engine version.
  - The major version should be 4 or higher.
- Install the SolarWinds SDK if you have not yet installed it:
  - Download the OrionSDK.msi installer from GitHub.
  - Run the installer and complete the setup wizard.
- Learn the basics of using the SolarWinds SDK in PowerShell.

- In PowerShell, add the SwisSnapin if you have not yet added it:
    - Add the SwisSnapin by running the Add-PSSnapin cmdlet: `Add-PSSnapin -Name SwisSnapin`

  For more information, open the SolarWinds SDK PowerShell page and follow the steps in the "Using SwisSnapin" section.

Get started with the API

ⓘ This section provides instructions on how to use Windows PowerShell, although you can also use Python OrionSDK to call to the API.

1. Open Windows PowerShell ISE to test the example(s).

   Enter Windows-key+R to open the Run dialog.

   Type powershell ise and press OK.
2. In PowerShell ISE, create a SWIS connection object using the Connect-Swis cmdlet.

   For details, open the SolarWinds SDK PowerShell page on GitHub and follow the steps in the "Cmdlets Provided by SwisSnapin" section.
3. In PowerShell ISE, enter the IPAM API cmdlets and run them. See the IPAM API reference for documentation.

IPAM status icons

In IPAM, network components are represented by colored icons indicating the extent to which each component is used, as shown in the following table.

Icon	Component	Status	Status Description
📁	Group	Used (Closed)	The group is closed, but it contains at least one other component (group, subnet, or supernet).
📂	Group	Used (Opened)	The group is open, and it contains at least one other component (group, subnet, or supernet).
IP🟢 Green	IP Address	Available	All addresses in defined groups, subnets, and supernets are, by default, considered Available unless they are typically reserved, as in the case of the network and broadcast addresses, or until they are otherwise assigned.
IP🟣 Purple	IP Address	Reserved	Typically, in subnets defined to contain more than two IP addresses, the smallest address—the network address—identifies the subnet to the rest of the network and the largest address—the broadcast address—is used to communicate to all addresses within the subnet. Both addresses are considered to be Reserved for a defined subnet.

Icon	Component	Status	Status Description
IP ● Cyan	IP Address	Transient	Addresses that are dynamically assigned to devices that may power on and off regularly or that may enter and exit the network frequently are designated as Transient.
IP ● Yellow	IP Address	Used	Any address currently assigned to a monitored device is considered Used.
IP ● Grey	IP Address	API Blocked	This indicates that the status is being modified by the API
⚠ Red	Subnet	Critical	At least 80 percent of all possible addresses in the subnet are designated as Used.
⚠ Yellow	Subnet	Warning	60 to 80 percent of all possible addresses in the subnet are designated as Used.
● Green	Subnet	Good	Less than 60 percent of all possible subnet addresses are designated as Used.
● Red	Supernet	Critical	At least 80 percent of all possible addresses in the supernet are designated as Used.
● Yellow	Supernet	Warning	60 to 80 percent of all possible addresses in the supernet are designated as Used.
● Green	Supernet	Good	Less than 60 percent of all possible addresses in the supernet are designated as Used.
● Green	DHCP Scope	Good	Less than 60 percent of all possible addresses in the Scope are designated as Used.

Icon	Component	Status	Status Description
⊗ Grey	DHCP Scope	Unreachable	DNS Scope is unreachable.