GETTING STARTED GUIDE

# IP Address Manager

Version 2020.2

solarwinds

Last Updated: Wednesday, June 3, 2020

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

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.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

# Table of Contents

**IPAM Getting Started Guide** ..... **4**

Contents ..... 4

**How do I get started with SolarWinds IPAM?** ..... **5**

**Populate IPAM with IP addresses** ..... **7**

Discover network devices ..... 7

Add discovered devices to SolarWinds IPAM ..... 11

Import IP addresses ..... 13

**Add a DHCP server** ..... **19**

**Add a DNS server** ..... **21**

**Create a DHCP scope** ..... **23**

**Reserve an IP address** ..... **24**

Make a reserved address available again ..... 25

**Create a subnet group** ..... **26**

**Grant a user read and write access to a subnet** ..... **29**

# IPAM Getting Started Guide

Welcome to the IPAM Getting Started Guide. This guide will take you from installation to full implementation of IPAM.

Download the PDF: PDF

## Contents


- How do I get started with SolarWinds IPAM?
- Populate IPAM with IP addresses
- Discover network devices
- Add discovered devices to SolarWinds IPAM
- Import IP addresses from a spreadsheet
- Add a DHCP server
- Add a DNS server
- Create a DHCP scope
- Reserve an IP address in a DHCP scope
- Create a subnet group
- Grant a user read and write access to a subnet

# How do I get started with SolarWinds IPAM?

SolarWinds IP Address Manager (IPAM) provides integrated DHCP and DNS administration, and IPv4 and IPv6 address management from the SolarWinds Orion Web Console.

IPAM administration features include:

- Centralized IP address management
- Unified DHCP and DNS management
- Web-based reporting and alerting
- Extended API support for IPv4
- Amazon Route 53 and Azure DNS monitoring
- IP address requests

For information about IPAM administration features, see the IPAM Administrator Guide.

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

Use this guide to configure SolarWinds IPAM, and add your devices to IPAM to manage and monitor your IP addresses, DHCP servers and scopes, DNS servers, and DNS zones.

**Customers:** Follow the recommendations in this guide to ensure your system capabilities are correct and your production environment is sized correctly. Minimum system requirements used during evaluation are not sufficient for a production environment. Access your licensed software from the SolarWinds Customer Portal. If you need any implementation help, contact our Support Team.

**Evaluators:** If you are evaluating SolarWinds IPAM, download a free 30-day evaluation. The evaluation version of SolarWinds IPAM is a full version of the product, functional for 30 days. After the evaluation period, you can convert your evaluation license to a production license. For assistance, contact sales@solarwinds.com.

Getting started with SolarWinds IPAM involves the following tasks:

☐ **Install SolarWinds IPAM.**

Use the SolarWinds Orion Installer to install IPAM. This is an all-in-one application that provides an easy-to-follow installation path for your environment, and guides you through every product installation and upgrade for all your SolarWinds Orion platform products.

| | |
|---|---|
| ☐ | **Discover your devices.**<br><br>Use the Network Sonar Discovery wizard discover network device, or use the Import wizard to manually import IP addresses and subnets. |
| ☐ | **Add discovered devices to SolarWinds IPAM.**<br><br>Use the wizard to select the discovered devices you want to monitor with IPAM. |
| ☐ | **Add DNS and DHCP servers.**<br><br>Integrate DHCP or DNS servers with IPAM to manage all of your servers through one interface. |
| ☐ | **Reserve an IP address in a DHCP scope.**<br><br>Reserve IP addresses in a DHCP scope to ensure a device receives the same IP address every time your servers reboot. |
| ☐ | **Create a subnet group.**<br><br>Create a subnet group to organize and manage a defined set of IP addresses. |
| ☐ | **Grant a user read and write access to a subnet.**<br><br>Restrict user access to help maintain security without limiting your ability to delegate required network management activities. |

Ensure your long-term success with IPAM by following the guidelines in this document. Depending on your workload, getting started with IPAM should take you one week or less.

# Populate IPAM with IP addresses

This section includes the following topics:


- Discover network devices
- Add discovered devices to IPAM
- Import IP addresses from an Excel spreadsheet
- Add DNS and DHCP servers to IPAM


## Discover network devices

IP Address Manager (IPAM) is designed to be used as part of the SolarWinds Orion Platform suite of products or as a standalone application. If you are already using the Orion platform to monitor your environment, and have created a database of nodes and associated elements, you can skip this section and start adding nodes for IPAM monitoring.

Discovery is the process SolarWinds Orion uses to identify network elements.

> The tabs shown as you proceed through the wizard depend on the SolarWinds Orion products you have installed. Click Next to move to the next tab.

1. Launch the Orion Web Console using either of the following methods:
   - Start the Orion Web Console from the SolarWinds Orion program folder.

   Or:

   - Launch a browser and enter:

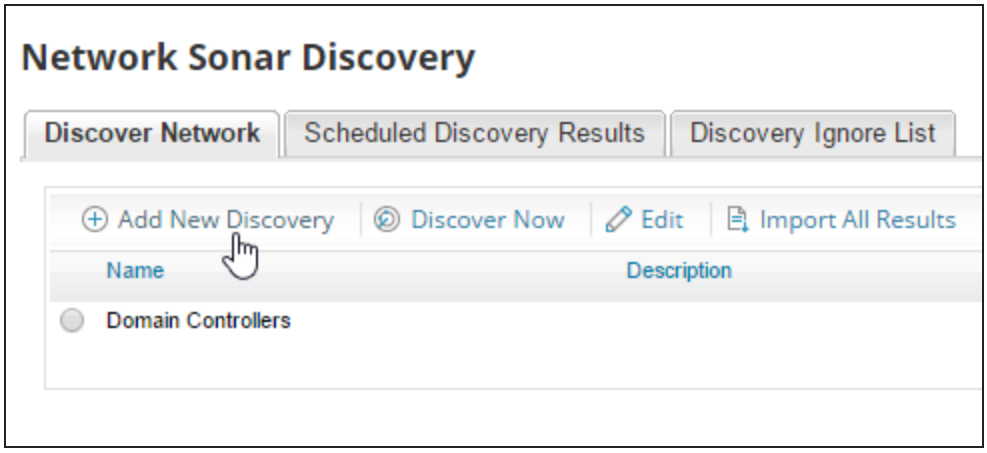
     `http://ip_address`

     or:

     `http://hostname`

     where *ip_address* is the IP address of your SolarWinds Orion server, and *hostname* is the domain name of your SolarWinds Orion server.
2. Log in with your username and administrator password.

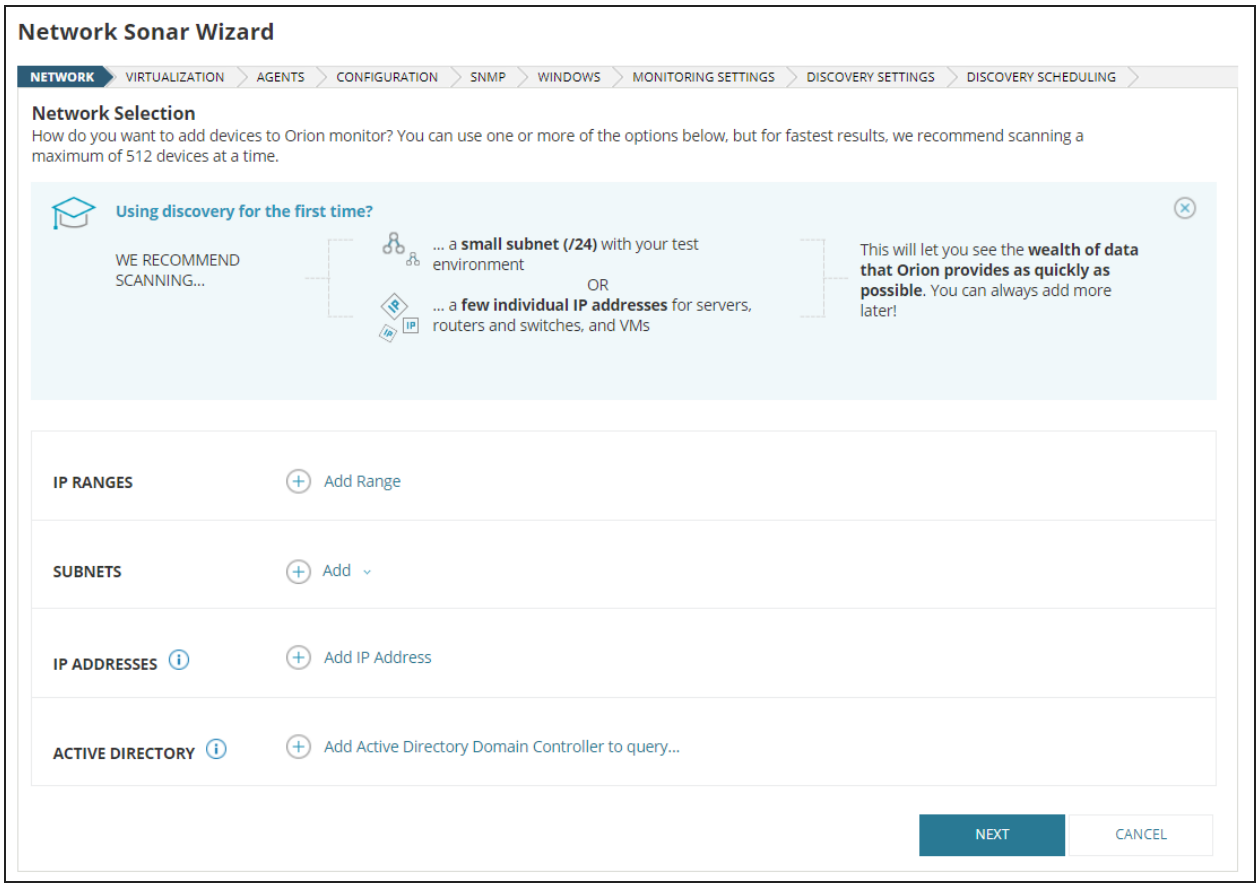
3. If the Network Sonar Discovery page is displayed, click Add New Discovery.




ⓘ If the Discovery wizard is not displayed, click Settings > Network Discovery

4. On the Welcome to Orion Web Console page, click Start.

   The Network Sonar wizard is displayed.



> ⓘ The tabs displayed on the Network Sonar wizard depend upon the SolarWinds products you have installed.

This wizard enables you to discover devices in several ways:

- Enter a range of IP addresses to monitor
- Enter a list of IP addresses
- Add nodes by querying your Active Directory Domain Controllers
- Enter a subnet or seed router IP address

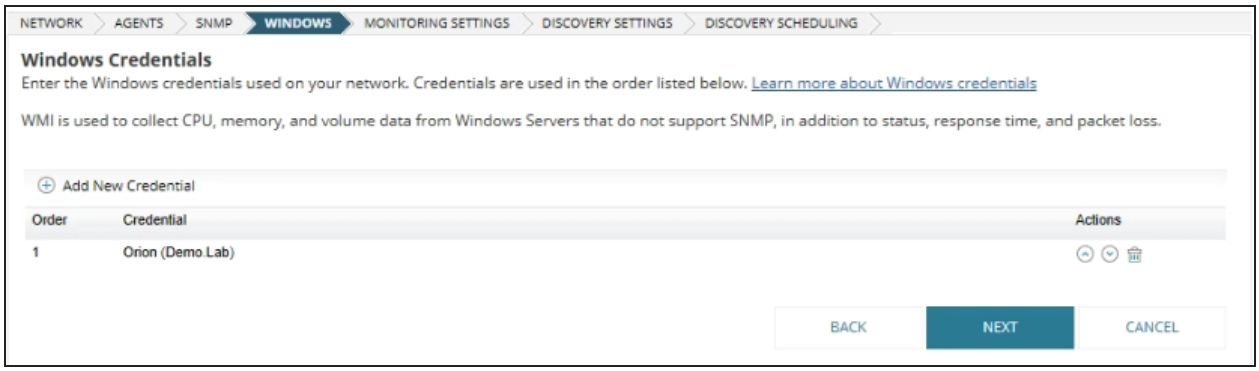
The easiest method when starting is to supply a range of IP addresses.

> ⓘ For instructions on using Active Directory Domain Controllers instead, see Discovering devices using Active Directory Domain Controllers.

6. Click Add Range.
7. Enter the start and end IP addresses you want to monitor, and click Next.
8. On the Agents tab, check the box if you want to check all nodes currently being polled using agents for changes updates, and click Next.
9. On the SNMP tab:
   a. If all devices on your network require only the default SNMPv1 and SNMPv2 public and private community strings, click Next.
   b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required information, and click Next.

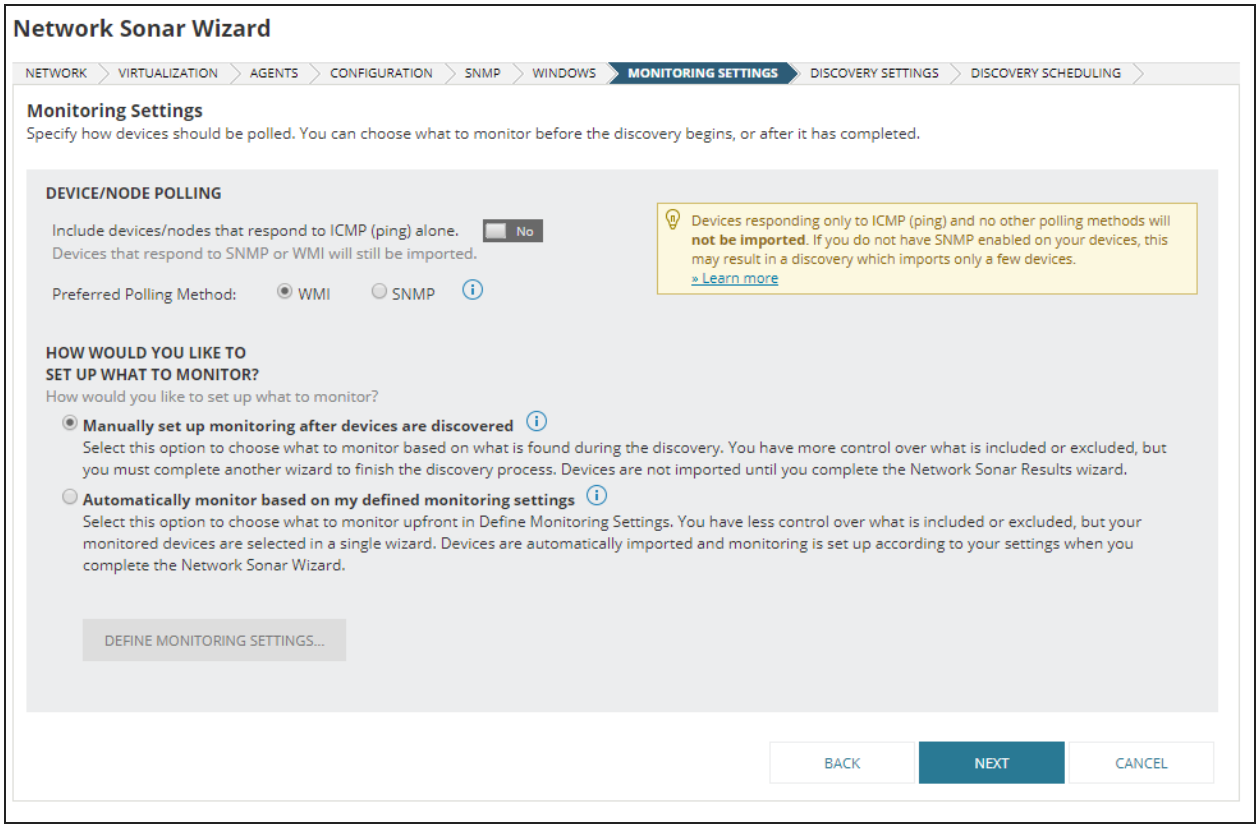
> ⓘ If you have an SNMP service enabled on a Windows server, SNMP credentials do not retrieve information for DHCP and DNS management.

10. On the Windows Credentials tab, click Add New Credential and provide the required information if you want to discover Windows devices that do not support SNMP, or want to collect additional information that SNMP does not poll.



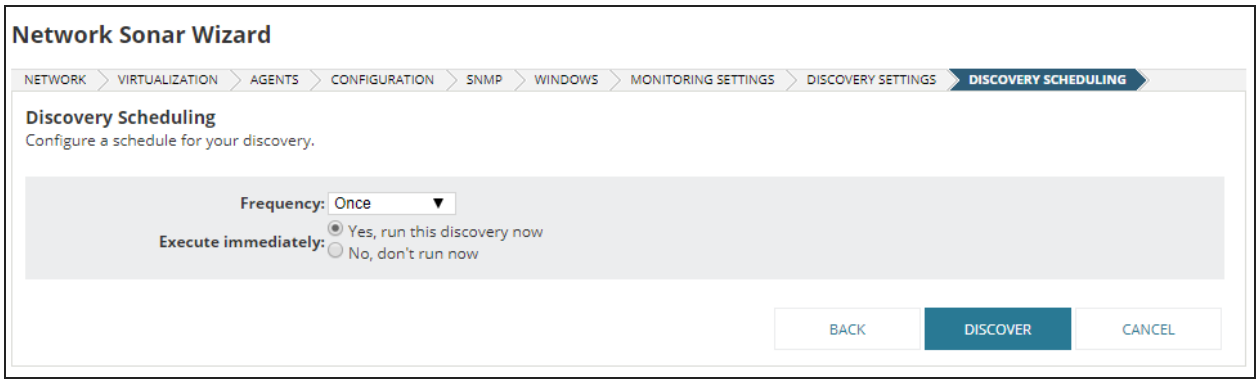

> SolarWinds recommends that you monitor Windows devices with WMI rather than SNMP to obtain this extra information.

11. On the Monitoring Settings tab, SolarWinds recommends manually setting up monitoring the first time you run discovery. This enables you to review the list of discovered objects and select only those you want to monitor (rather than automatically monitoring them all).




12. On the Discovery Settings panel, enter a name and description for this discover, and click Next.
13. Accept the default frequency and run the discovery immediately.

> Once you are satisfied with the discovery settings you can add a frequency on this tab to run this discover according to a schedule.




Discovery can take anywhere from a few minutes to a few hours, depending on the number of network elements the system discovers. After discovery is complete, you can add the discovered devices using the Network Sonar Results wizard.

# 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 Orion database. Discovered elements do not count against your license count; only elements that are imported into the Orion 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.

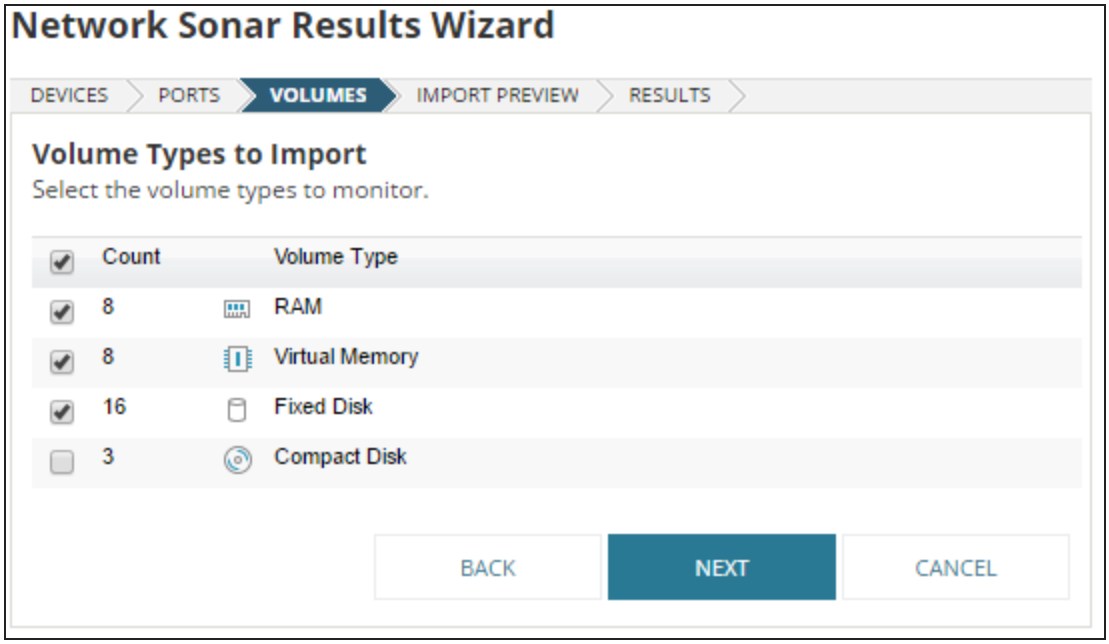
1. Ensure that only the device types you want to monitor are selected, and click Next.

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

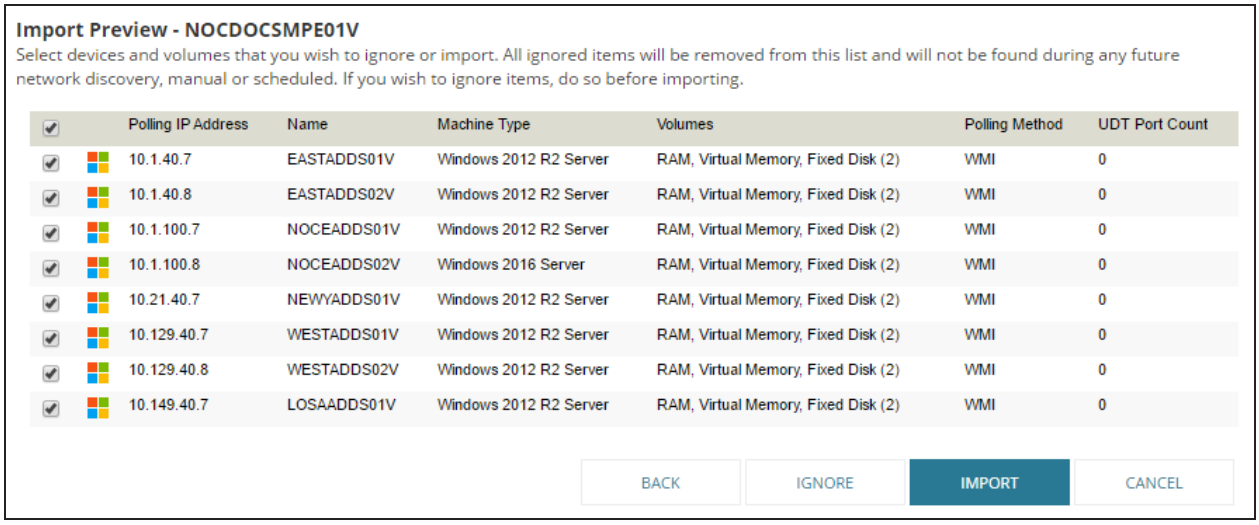
> ⓘ The Ports tab is only available if you have SolarWinds Orion User Device Tracker (UDT) installed.

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.



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




| 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, click Finish on the Results panel.
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 | | | | |

IPNode

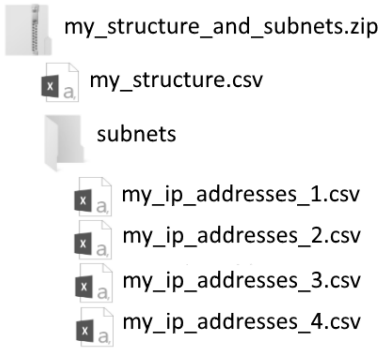
For a structure spreadsheet, only the Type of each object needs to be provided. This can be Group, Supernet, Subnet, IPv6Subnet, GlobalPrefix, PrefixAggregate, etc.

| | 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 |

subnets

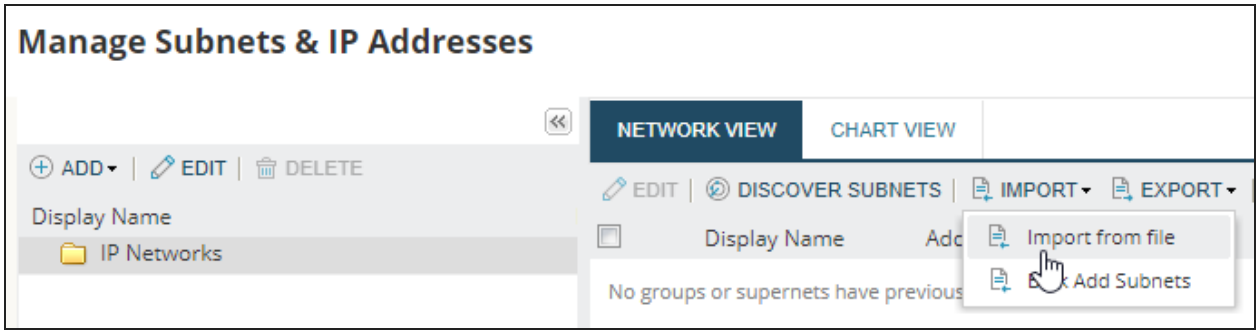
Subnet or Structure spreadsheets can be imported as individual .csv, .xls, or .xlsx files.

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.




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.




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.

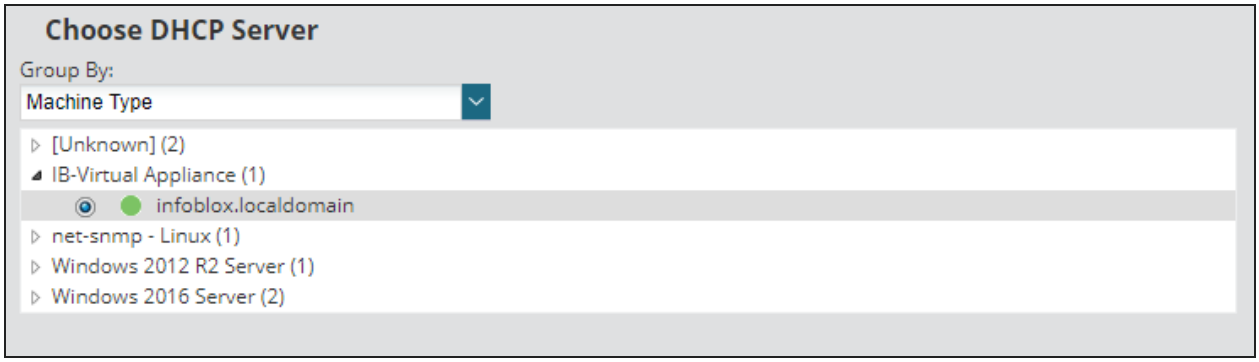
   - Click Assign IPs to Existing Subnets to add addresses to subnets that have already been created.

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

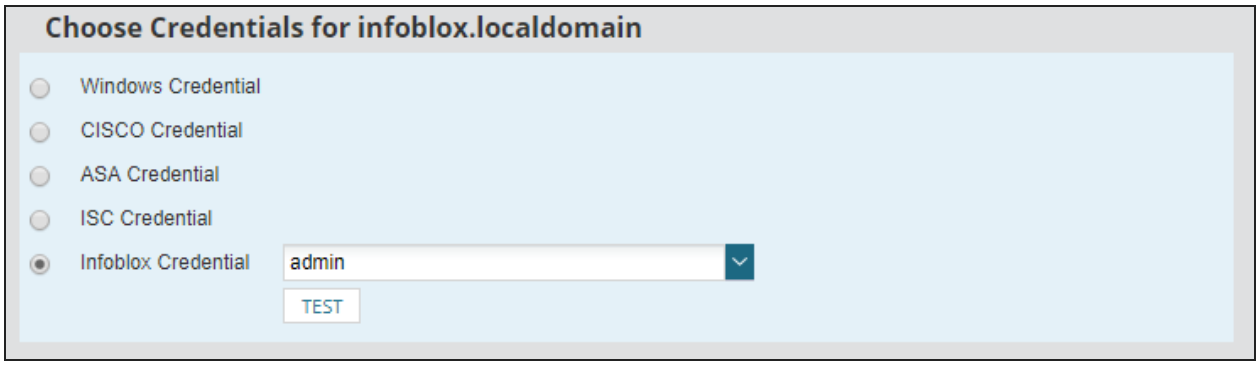
# Add a DHCP server

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

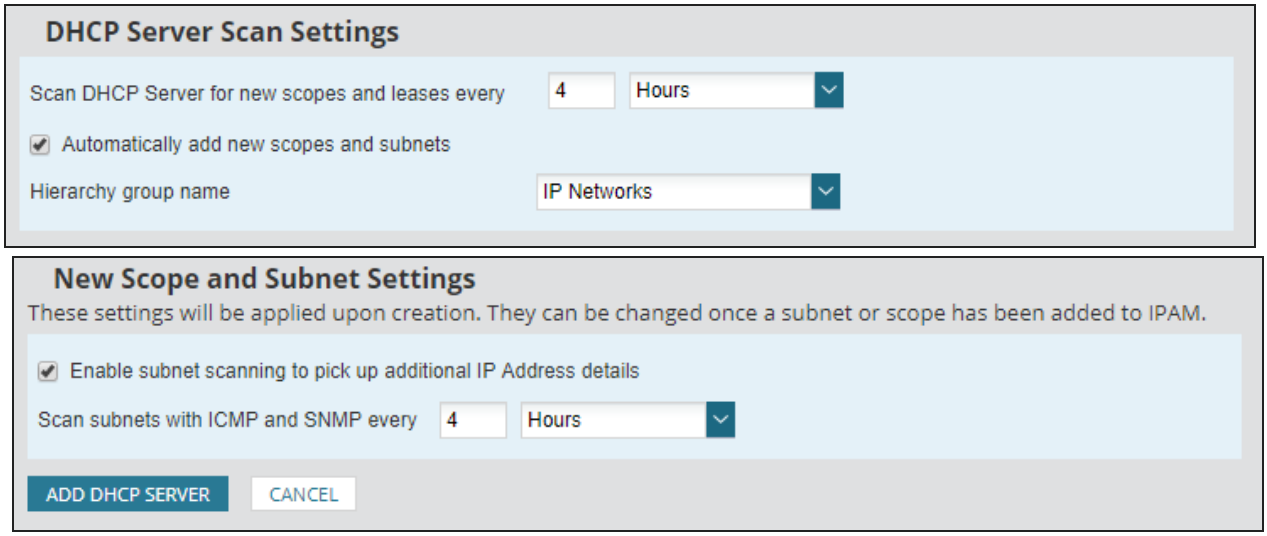
1. Navigate to Settings > All Settings.
2. Click IPAM Settings in the Product Specific Settings section.
3. Click Add DHCP Server in the DHCP & DNS Management section.
4. Select the required server from the Choose DHCP Server drop-down menu.



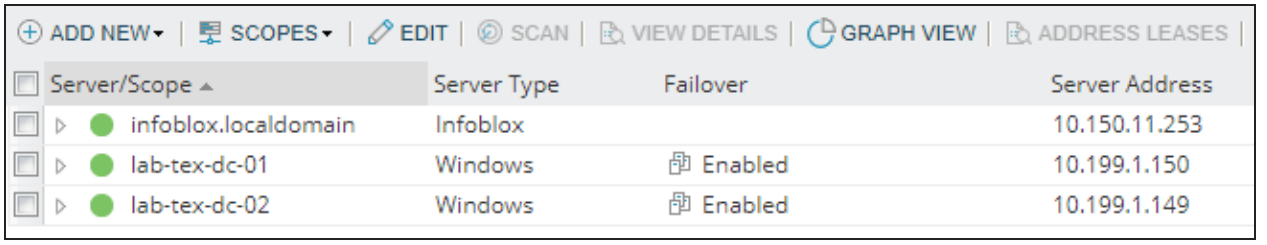

5. Select a credential type, and enter the credential details.
6. Click Test. If the credential are valid for the selected server the Test Successful message will be displayed.



7. Select your default DHCP Server Scan Settings, and click Add DHCP Server.




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

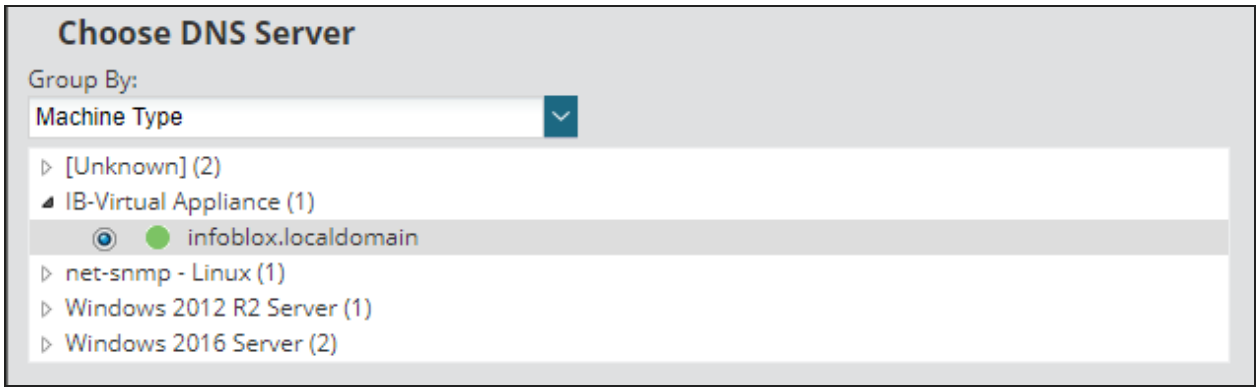


# Add a DNS server

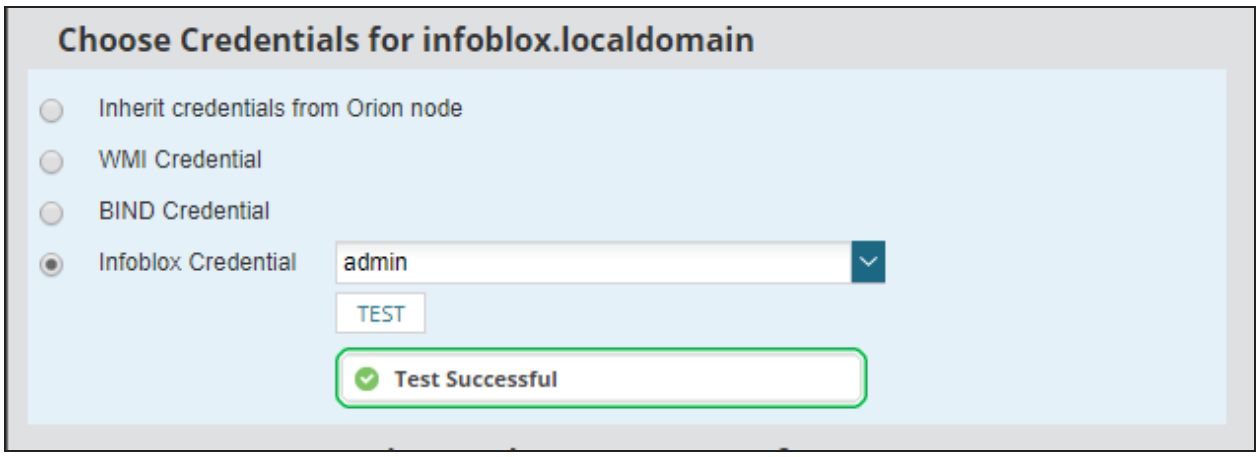
A DNS server translates your numeric IP addresses to domain names and host names. When a domain name is called, IPAM scans all DNS servers to search for its IP address.

1. Click My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DNS Server tab, click Add New, and select DNS Server.
3. Select a DNS Server.

   Use the Group By menu to select a method for sorting DNS servers.




4. Depending on the DNS server type, either use the credential from the Orion node, or select the appropriate credential type and supply the credential.

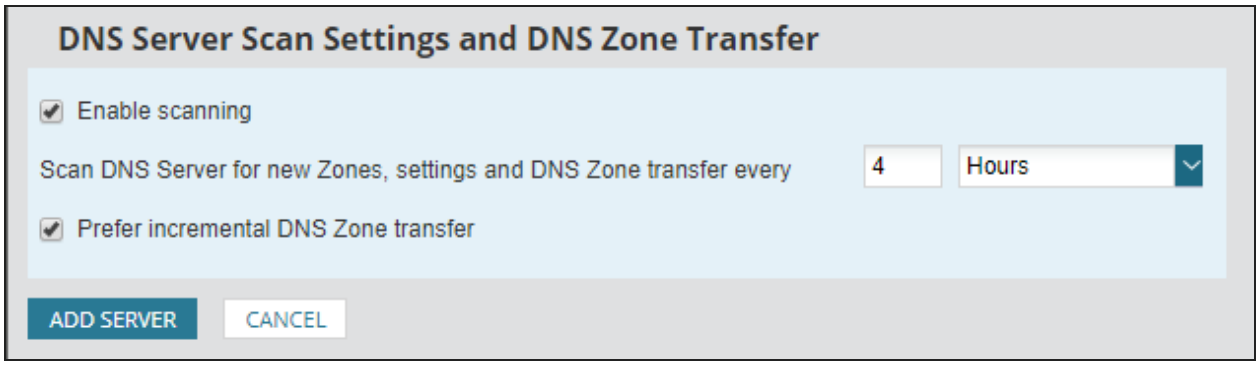



5. Click Test. If the credential are valid for the selected server the Test Successful message will be displayed.

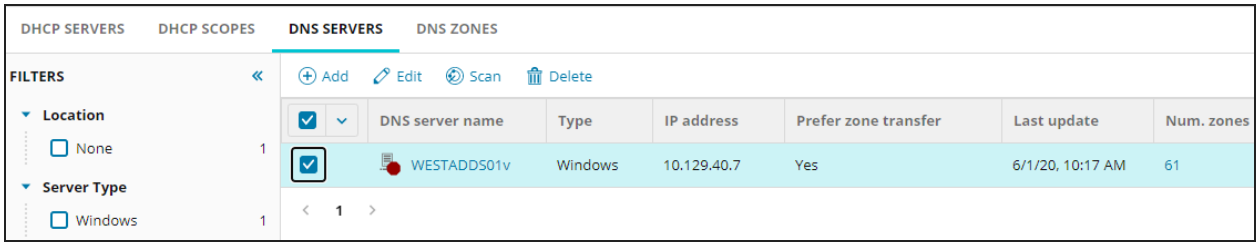
6. Select Enable Scanning to enable incremental DNS Zone transfers, and select the scan interval.

   IPAM will scan the DNS server for new zones and settings based upon this interval time.

7. Click Add Server.




The DNS server is added to the DHCP & DNS Management page and begins scanning domain and host name exchange activity.



# Create a DHCP scope

A DHCP scope is a predefined range of IP addresses for a subnet that the DHCP server is configured to dynamically allocate to DHCP clients. In the simplest setup, a DHCP server would serve a single scope which would correspond to a subnet. However, you may need to create scopes that are smaller than a subnet or that have exclusions.

Reasons for excluding IP addresses from scopes include:

- The computer running the DHCP server may require a static IP address assignment.
- Some devices may not support DHCP, and require a static IP address.

Before you can create a scope, you will need to know the start and end IP address for the scope.

1. Click My Dashboards > IP Addresses > DHCP & DNS Management.
2. Select the DNS Server for which you want to create this scope.
3. Enter a name for the scope, and any additional details if available, and click Next.
4. Enter the start and end IP addresses for the scope, and click Next.
5. Leave the DHCP Offer Delay as 0 ms and click Next.

   The Offer Delay setting is used if you have more than one DHCP server for this scope, and want to specify the order in which servers respond to client requests. By setting the Primary DHCP to 0 milliseconds and the Secondary to 1000 milliseconds you will assure that the Primary DHCP server is used unless unavailable.

6. Add any DHCP Option required, and click Next.

   If you click Add New Option, the Choose DHCP Options window is displayed listing the options and giving a brief explanation of each.

   For example, you may want to set a lease duration. This specifies how long an IP address is initially allocated to a client. For a stable environment where devices are not regularly added or replaced, this can safely be increased beyond the default of 8 days. For networks that include transitory wireless devices such as laptops, you might want set this to an hour.

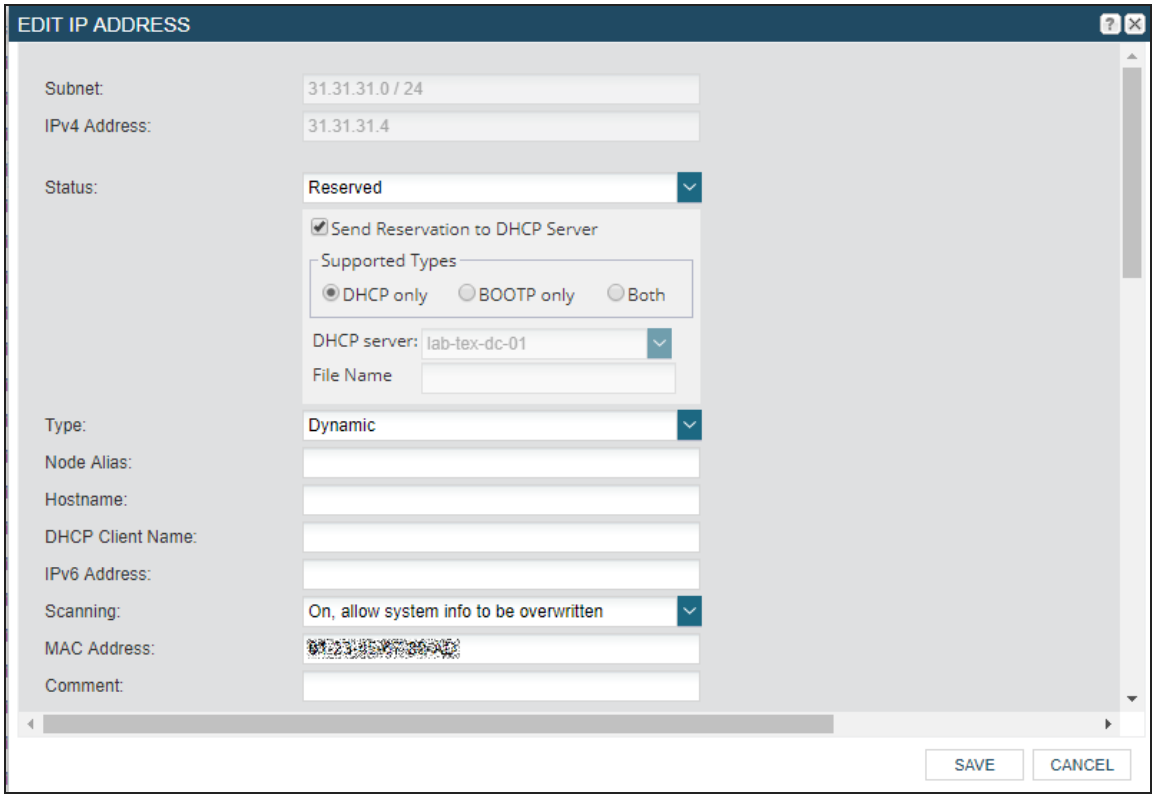
7. Click Create Scope.

# Reserve an IP address

You can reserve an IP address in a DHCP scope to ensure a device receives the same IP address every time your server reboots and the device is detected.

1. Click My Dashboards > IP Addresses > DHCP & DNS Management.
2. Expand the DHCP servers and click a scope to view the IP address details. This shows the current status of the IP addresses in the scope. Available IP addresses are green.
3. Select the IP address that you want to reserve, and click Edit.

   The Edit IP Address window is displayed.




4. Select Reserved from the Status drop-down.
5. Check the Send Reservation to DHCP Server box.

   > ⓘ If you do not check this box, the reservation will only be made in the IPAM database, not on the DHCP server.

6. Select the type: Dynamic or Static.
7. Enter a hostname for the device in the DHCP Client Name field.

8. Enter the MAC Address of the device for which you want to reserve this IP address.
9. Click Save.

   This IP address is now reserved for this device, and will be assigned to it when the device is detected on the network.

## Make a reserved address available again

If you no longer need to reserve this address, change the Reserved status to Available to free the IP address for active devices.

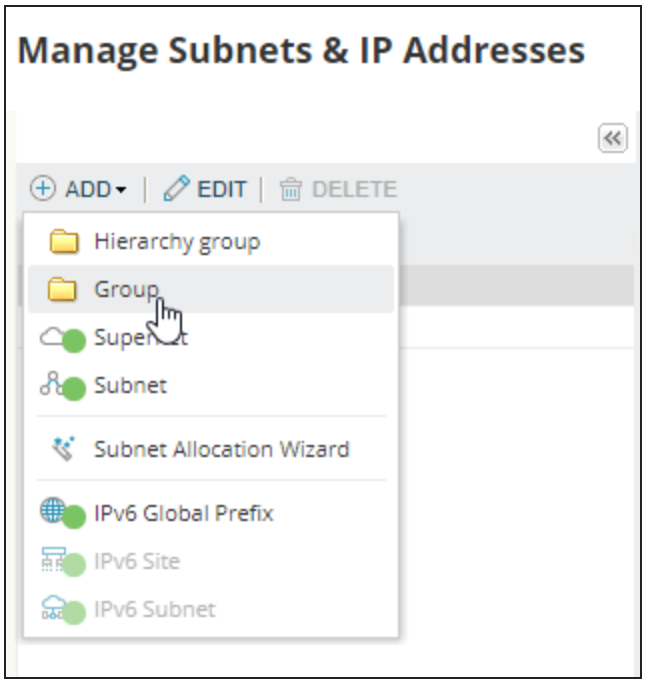
1. Follow the steps above to step 3, selecting the reserved address.
2. Select Available from the Status drop-down.
3. Click OK.

   The data fields for the associated device are blanked out.
4. Check the Remove Reservation box.
5. Click Save.

# Create a subnet group

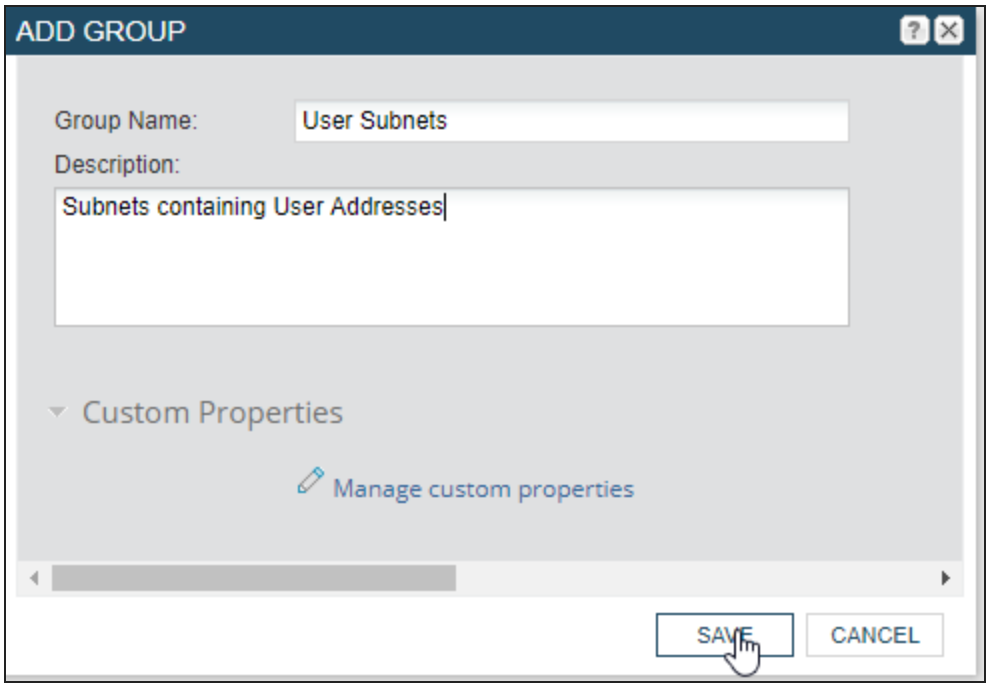
Grouping subnets helps you better organize and manage a defined set of IP addresses. You can monitor server status and availability and IP address static assignments within groups. Administrators can also edit, move, and export subnet groups.

1. Click My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Click Add > Group.

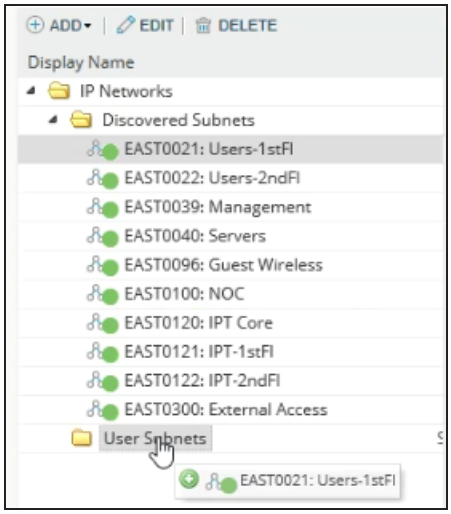



3. Enter a Group Name and Description, and click Save.

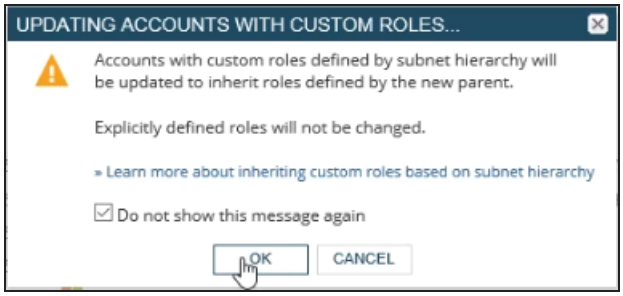
   A User Subnets child folder is created under the IP Networks parent folder.



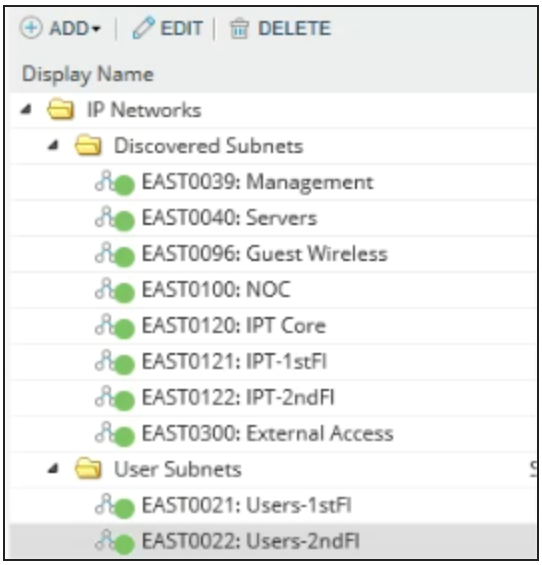

4. Select the subnets and drag and drop into the User Subnets folder.




5. On the Updating Accounts dialog box, click OK.



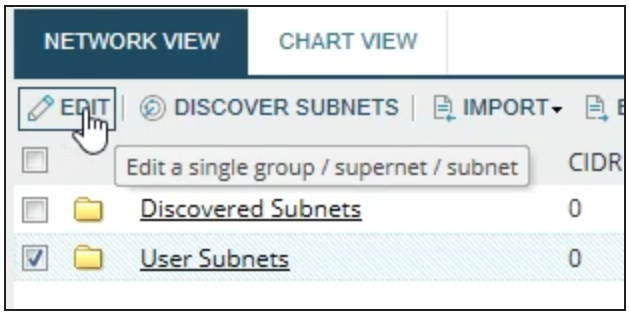

All subnets that contain user IP addresses are now grouped into the User Subnets folder for easy access.


ADD
EDIT
DELETE
Display Name
IP Networks
Discovered Subnets
EAST0039: Management
EAST0040: Servers
EAST0096: Guest Wireless
EAST0100: NOC
EAST0120: IPT Core
EAST0121: IPT-1stFl
EAST0122: IPT-2ndFl
EAST0300: External Access
User Subnets
EAST0021: Users-1stFl
EAST0022: Users-2ndFl

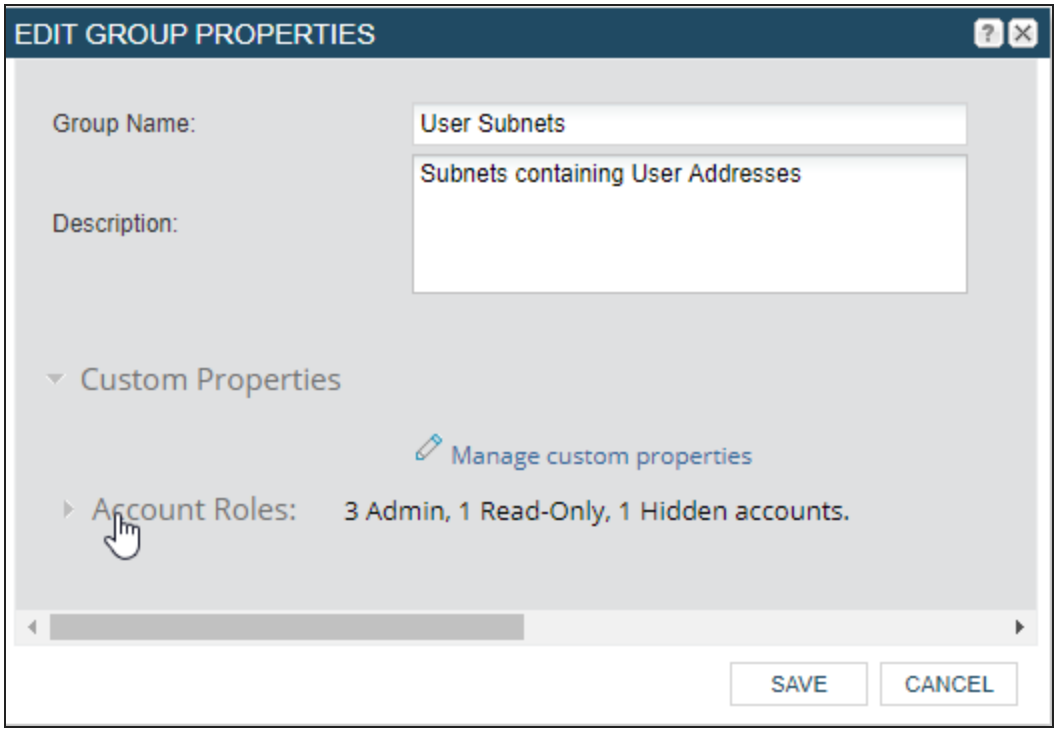
# Grant a user read and write access to a subnet

Use role definitions to restrict user access to a subnet to help maintain security without limiting your ability to delegate required network management activities. This topic grants read and write permissions to the User Subnets folder created in the Create a subnet group topic.

1. Go to My Dashboards > IP Addresses > Manage Subnets & IP Addresses.
2. Select a subnet, supernet, or group, and click Edit.

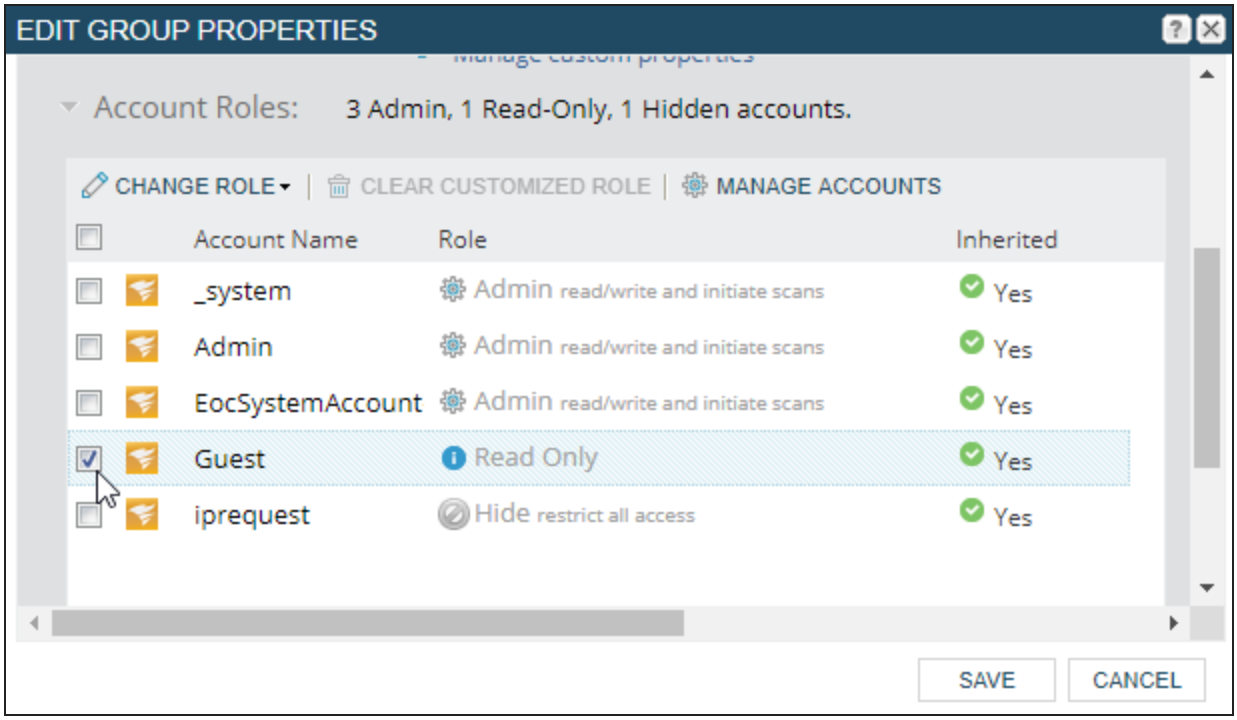



3. In the Edit Group Properties window, click Account Roles.

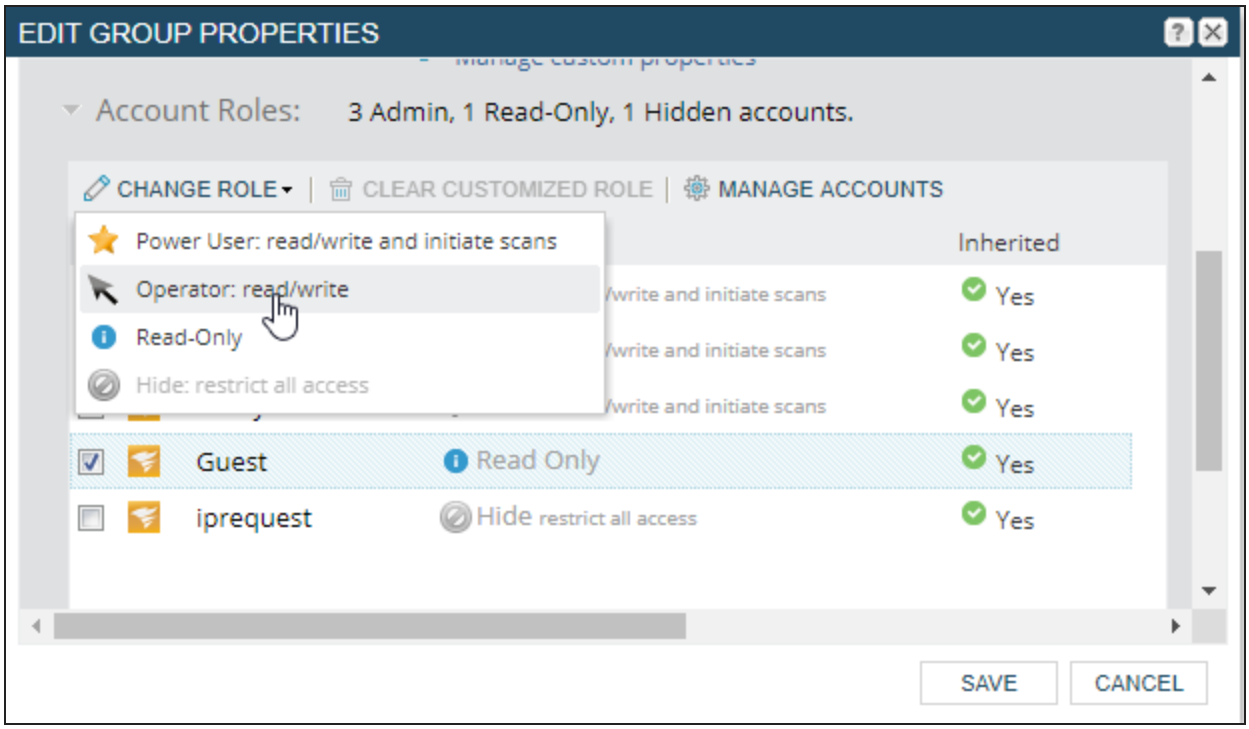



To verify a user's permissions, view the Account Roles of a user.

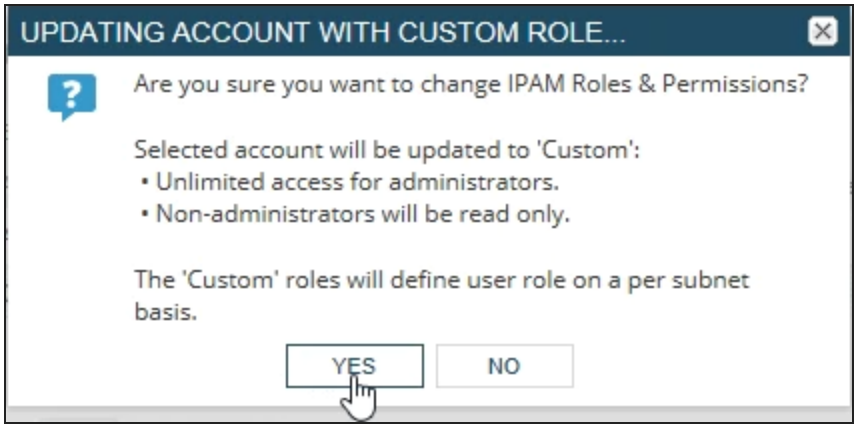
4. Select an Account Name.

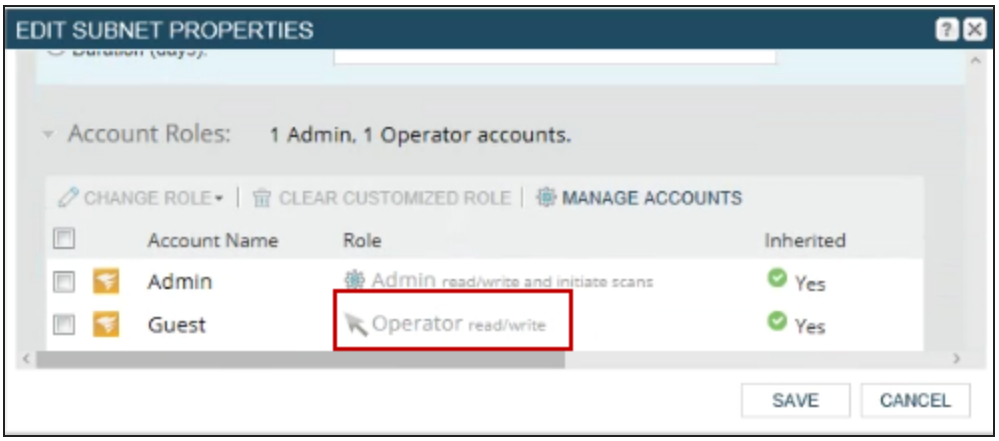



5. Click Change Role > Operator: read/write.



6. Confirm the selection, and click Yes.




7. Click Save.

The Guest user now has access to make read and write updates to the User Subnets.