SolarWinds

IP Address Manager
Evaluation Guide

solarwinds

Unexpected Simplicity

Version 4.2, revised 8.26.2014

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	sales@SolarWinds.com www.SolarWinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.SolarWinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
Italics	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you

Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1|value2	Exclusive command parameters where only one of the options can be specified

SolarWinds Orion IP Address Manager Documentation

The following documents are included in the SolarWinds Orion IP Address Manager documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Evaluation Guide	Provides an introduction to Orion Network Performance Monitor features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the Orion IP Address Manager user interface
Release Notes	Provides the latest information about known issues, and updates. The latest Release Notes can be found at www.SolarWinds.com.

Table of Contents

Chapter 1: Introduction

IP Address Manager (IPAM) leverages an intuitive web interface to allow you to easily investigate IP address space issues. By scanning the network for IP address changes, IPAM maintains a dynamic list of IP addresses and allows engineers to plan for network growth, ensure IP space usage meets standards, and helps troubleshoot IP addressconflicts.

IPAM also allows you to manage and monitor your DHCP & DNS servers. Windows, Cisco ,ASA, BIND, and ISC are currently supported.

- For more DHCP information see the following: DHCP Management
- For more DNS information see the following: DNS Management

What's New in IPAM

IP Address Manager version 4.2 features:

- Automatic Subnet Discovery - A new discovery wizard creates subnet structures and imports them into IPAM for monitoring.
- Device fingerprinting - MAC address to vendor in the IP Address Details View
- DNS A & PTR Record Pairing - DNS Forward & Reverse Mismatches display in the web.
- Improved search capabilities
- Improved scope utilization views
- IPv6 Discovery of IPv6 addresses - IPAM polls and updates the status of each IPv6 address added by scanning and status history using Neighbor Discover Protocol

Previous Versions Release Features:

Version 4.1 features:

- ISC DHCP management and performance monitoring
- A new re-designed DHCP management UI that helps to manage multiple methods of organizing IPs across Windows, CISCO and ISC DHCP vendors.
- Management of ISC DHCP specific subnet options, ranges and pools.
- Monitoring of ISC shared network containers and their subnet utilization.
- Monitoring of ISC DHCP IP address static assignments within groups.
- Cisco & Windows DHCP Options Support
- Monitor and manage over 180 (RFC 2132) DHCP options on Cisco, Microsoft and ISC DHCP server.
- This release also includes new UI for DHCP options management with data type validator and text translation of numeric value of each option (you don't have look into RFC doc.)

How IPAM Works

Using ICMP and SNMP calls to collect details from devices on your network, IPAM tracks and displays IP address usage, in addition to automatically marking IP addresses that are no longer in use.

Additionally, WMI calls to DHCP and DNS servers are made to retrieve lease and scope details. Data is stored for tracking and auditing purposes in the database. All statistics are accessible using the Orion web interface.

There are 3 scanning modes used to scan IP addresses.

- ICMP scan (ping sweep)
- SNMP scan
- Neighbor scan (using ARP tables)

Networking Concepts and Terminology

The following sections define the networking concepts and terminology that are used within IPAM. Some IPAM terms correspond specifically to status icons. For more information about the icons used in IPAM, see "IPAM Status 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 and broadcast addresses. In IPAM, available IP addresses are indicated with a gray IP icon. For more information, see "IPAM Status Icons".

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, with the leading bits of the binary expansion underlined, 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
Note: 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 **214.100.00.45/16** 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, **214.100.48.45/20**, as revealed when the two addresses are expressed in binary, as follows, where the twenty leading bits, which are identical, are underlined:

11010110.01100100.00110010.00000100 = 214.100.50.04
11010110.01100100.00111101.00101101 = 214.100.61.45

11010110.01100100.00110000.00000000 = 214.100.48.45/20

Group

In Orion IPAM, groups serve as containers for the subnets, supernets, and even other groups you define to organize and manage your network. For more information about creating and using groups in Orion IPAM, see “Managing Groups in IPAM”.

Reserved

Typically, in subnets defined to contain more than 2 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 the network address and the broadcast address are considered to be **Reserved** for a defined subnet. In Orion IPAM, reserved IP addresses are indicated with a purple IP icon. For more information, see “IPAM Status Icons”.

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, which are identical, are underlined:

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. For more information about creating and managing subnets in Orion IPAM, see “Managing Subnets in IPAM”.

Supernet

A supernet is an element of network organization consisting of contiguous CIDR blocks, or subnets. In networks with well-defined subnets, supernets allow network administrators to consolidate and limit IP traffic 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, where the underlining highlights the common address bits of the supernet.

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 like laptops or some user workstations
- devices that enter and exit the network frequently, like laptops on a wireless network
- any devices on a DHCP-enabled network

Note: 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. For more information, see “IPAM Status Icons”.

Used

The **Used** label is provided to indicate any IP address that is currently assigned and not otherwise available. For more information, see “IPAM Status Icons”.

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).
 Grey	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.
 Purple	IP Address	Reserved	Typically, in subnets defined to contain more than 2 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.
 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.
 Yellow	IP Address	Used	Any address currently assigned to a monitored device is considered Used.
 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

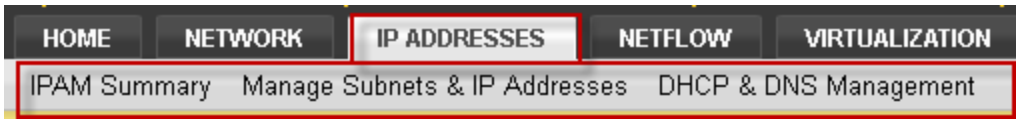
			designated as Used.
 Yellow	Supernet	Warning	60 to 80 percent of all possible addresses in the supernet are designated as Used.
 Green	Supernet	Good	Less than 60 percent of all possible addresses in the supernet are designated as Used.
 Red	DHCP Scope	Critical	At least 80 percent of all possible addresses in the Scope are designated as Used.
 Yellow	DHCP Scope	Warning	60 to 80 percent of all possible addresses in the Scope are designated as Used.
 Green	DHCP Scope	Good	Less than 60 percent of all possible addresses in the Scope are designated as Used.
 Disabled	DHCP Scope	Disabled	DHCP scope is currently disabled.
 Unreachable	DHCP Scope/Zone	Unreachable	DNS Scope/Zone is unreachable.

Understanding the IPAM Website

The IP Address Manager view is the interactive center of your managed IP network.

The IPAM website consists of three primary tabs:

- IPAM Summary
- Managing Subnets & IP Addresses
- DHCP & DNS Monitoring



IP Address Manager Summary View

The following sections describe the default resources available on this view for managing your network.

Top 10 Subnets by % IP Address Space Usage

The Top 10 Subnets by % IP Address Space Usage resource provides an easily accessible report of IP address availability by defined subnet. Defined subnets are listed in decreasing order of IP address space percentage used (**% IP Address Space Used**). For each defined subnet, this resource provides a colored bar graph indicating the percentage of the total IP address space of your network that is currently in use or reserved. To provide further detail, this resource displays both the number of IP addresses designated for a selected subnet (**IPs Used**) and the number of IP addresses currently available for assignment (**IPs Available**) such that the **% IP Address Space Used** value is calculated as follows:

$$\%\text{IP Address Space Used} = \frac{\text{All IPs in Subnet} - \text{IPs Available}}{\text{All IPs in Subnet}}$$

Top 10 DHCP Scopes by % IP Address Space Usage

This view displays the Top XX DHCP Scope availability. Defined Scopes are listed in decreasing order of IP address space percentage used (**% IP Address Space Used**). For each defined Scope, this resource provides a colored bar graph representing the percentage of IP address space available. To provide further detail, this resource displays both the number of IP addresses designated for a selected subnet (**IPs Used**) and the number of IP addresses currently available for assignment (**IPs Available**).

Search for IP Address

The Search for IP Address resource allows you to search multiple fields within the Orion IPAM table of your Orion database for IP addresses you are managing with IPAM. For more information about searching the IPAM table of your Orion database, see “Searching for IP Addresses ”.

Custom List of Reports

The Custom List of Reports resource provides a list of selected Orion reports. Any report that is either predefined or subsequently created using Orion Report Writer may be listed in this resource. For more information about creating your own custom Orion IPAM reports, see "Creating Reports with IPAM".

To edit the displayed list of reports, click **Edit** in the resource title bar. The Edit Custom List of Reports page opens, and then you can select from available network reports to list in this resource and edit the resource Title and Subtitle.

Getting Started with IP Address Manager

This resource provides a quick method to get your environment configured to work with IPAM by providing quick links to set up credentials, import devices from the Engineer's Toolset, bulk add subnets and add DHCP servers to be monitored. Once completed, you can click Remove This Resource to remove this resource from appearing on the summary page.

Thwack Recent IPAM Posts

Thwack.com is the online SolarWinds community for network engineers. The thwack Recent IPAM Posts resource shows the most recent IPAM-related posts submitted by users to the IPAM forum.

Clicking the title of any listed post opens the corresponding thwack.com post in a new browser.

Clicking **Edit** gives you the option to set the **Maximum Number of Posts to Display** in the resource. Type the number of post titles you want to display in the resource, and then click **Submit**.

Clicking **View All** opens the thwack.com IPAM forum, where you can read all posts related to IPAM.

Manage Subnets and IP Addresses Page

The Manage Subnets and IP Addresses page is the primary management interface for IPAM. The page is divided into two panes. The left pane displays your entire managed network as it is organized into subnets, supernets and groups.

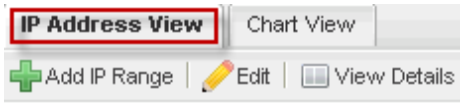
For more information about organizing your network with subnets, see "Managing Subnets in IPAM".

For more information about organizing your network with supernets, see "Managing Supernets in IPAM".

For more information about organizing your network with groups, see "Managing Groups in IPAM".

Depending on the current selection in the left pane, the right pane contains two tabs, each of which provides one of the following views: IP Address, Network, and Chart. The following sections describe the information that is available on each these Manage Subnets and IP Addresses views.

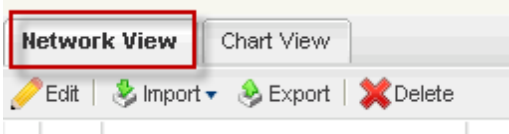
IP Address View



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 and 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 dropdown menu.

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. For more information about editing IP address properties, see "Adding IP Addresses".

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 and IP Addresses page. If a group is selected, this view provides a list of all other groups, supernets, and subnets that are defined within the selected group. If a supernet is selected, this 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, delete and import subnets by bulk.

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

For more information about network component icons, see "IPAM Status Icons".

Each network component (group, subnet, and supernet) is listed with a selection of component properties. 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. For more information about editing group, properties, see "Editing Groups".

For more information about editing subnet properties, see "Editing Subnets".

For more information about editing supernet properties, see "Editing Supernets".

Chart View

The Chart View is always available in the right pane of the Manage Subnets and IP Addresses page, and it provides a concise, visual report of your IP address allocation for any network component selected in the network organization pane to the left. A pie chart displays the designated statuses of your monitored IP addresses and 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.

For more information about IP address states in IPAM, see "IPAM Status Icons".

DHCP & DNS Monitoring Page

The DHCP & DNS Monitoring page is divided into two panes. The left pane displays your entire managed network as it is organized into Scopes or Servers. You can filter how these are grouped by using the drop down arrow.

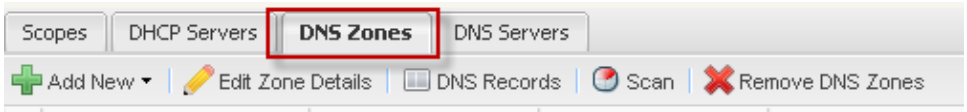
The right pane contains four tabs, each of which provides one of the following views: Scopes tab, DHCP Servers tab, DNS Zones tab, DNS Servers tab.

The following sections describe the information that is available on each these views.

DHCP Servers tab

The DHCP Servers View displays a list of all DHCP Servers that are monitored with IPAM. Click a Server to drill down to see the Scope View. Click a Scope to see the IP Address View details. For more information about editing DHCP Server properties, see "DHCP & DNS Monitoring Page".

DNS Zones tab



The DNS Zones tab displays all monitored DNS Zones. Information includes:

- Zone Status
- Zone Type Lookup Type
- DNS Server/Address
- Zone Transfer Preference
- Last Zone Transfer Time
- Dynamic Updates

DNS Servers Tab

The DNS Servers tab display all IPAM monitored DNS Servers. By default information included contains:

- Server Address
- Zone Transfer Preference
- Last update time
- Number of Zones
- Location VLAN ID
- Server Description

Chapter 2: Installing IPAM

This chapter includes information needed to install IPAM.

Installation

The following procedure guides you through the installation of Orion IPAM. Ensure that the server on which you install Orion IPAM meets or exceeds the stated requirements. Complete the following procedure to install Orion IPAM.

Note: If you have additional Orion pollers or Web Consoles, upgrade them at the same time as your Orion server.

To install IP Address Manager:

1.Log on to the server that you want to use for IP address management.

Note: Consider backing up your database before performing any upgrade.

2.Navigate to your download location and launch the executable.

3.Review the Welcome text, and then click **Next**.

4.Accept the terms in the license agreement, and then click **Next**.

5.Click **Next**, and then click **Finish**.

6.Click **Enter Licensing Information**.

7.***If the computer on which you installed IPAM is connected to the Internet,*** complete the following procedure.

a.Click **I want to activate my license over the Internet**.

b.Browse to **http://www.SolarWinds.com/customerportal/**.

c.Login to the customer portal using your CustomerID and Password.

d.Copy your IPAM Activation Key to the clipboard, and then paste it into the Activation Key field on the Activate IPAM window.

e.Click **Next**.

f.Enter your contact information.

g.***If you use a proxy server to access the Internet,*** check the Proxy Server checkbox, and then type the proxy address and port number.

h.Click **Next**.

8.When the Orion IP Address Manager Setup Wizard completes, click **Finish**.

9.***If the Configuration Wizard does not start automatically,*** click **Start > All Programs > SolarWinds Orion > Configuration Wizard**.

10.Review the Orion Configuration Wizard welcome text, and then click **Next**.

11.Confirm that all services that you want to install are checked in the Service Settings window, and then click **Next.**

12.Click **Finish** when the Orion Configuration Wizard completes.

IPAM employs a simple, wizard-driven install process allowing you to quickly start managing your network. Refer to the following sections for more information about licensing, system requirements and configuration procedures.

IPAM Installation Requirements

IPAM can be installed as a standalone product or as a module to Network Performance Monitor (NPM).

The module scenario above requires a minimum version of NPM 11.0.1

General Installation Requirements

SolarWinds recommends installing your Orion product on its own server, with the IPAM database hosted separately, on its own SQL Server. Installations of multiple IPAM servers using the same database are not supported.

Hardware Requirements

The following table lists minimum hardware requirements and recommendations for your Orion server.

Note: Hardware requirements are listed by Orion license level.

Hardware	IP1000, or IP4000	IP16000	IPLX

CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
	Note: Dual processor, dual core is recommended.		
Hard Drive Space	2 GB	5 GB	20 GB
	Note: A RAID 1 drive for server operating system, IPAM installation, and tempdb files is recommended. The installer needs 1GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on the same drive as your server operating system.		
Memory	3 GB	4 GB	4 GB
Application Ports	161/SNMP and 443/SNMP. VMware ESX/ESXi Servers are polled on 443. 17777/TCP open for Orion module traffic 17778/ HTTPS open to access the SolarWinds Information Service API		

Software Requirements

The following table lists minimum software requirements and recommendations for your server.

Software	Requirements
Operating System	Windows Server 2003 or 2008, 2012, including R2, with IIS in 32-bit mode. IIS must be installed, and Windows 2012. SolarWinds recommends that IPAM administrators have local administrator privileges to ensure full functionality of local Orion tools. Accounts limited to use of the IPAM Web Console do not require administrator privileges. Note: SolarWinds does not support production installations of Orion products on Windows XP, Windows Vista, or Windows 7

	systems.
Web Server	Microsoft IIS, version 6.0 and higher, in 32-bit mode. DNS specifications require that hostnames be composed of alphanumeric characters (**A-Z**, **0-9**), the minus sign (**-**), and periods (**.**). Underscore characters (**_**) are not allowed. For more information, see RFC 952. Note: SolarWinds neither recommends nor supports the installation of any Orion IPAM product on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.
.NET Framework	Version 3.5. .NET Framework 3.5 SP1 is recommended.
SNMP Trap Services	Windows operating system management and monitoring tools component
Web Console Browser	Microsoft Internet Explorer version 6 or higher with Active scripting Firefox 3.0 or higher (Toolset Integration is not supported on Firefox)

Big Iine SQL Database Requirements

The Orion Installation Wizard installs the following required x86 components if they are not found on your Orion database server:

- SQL Server System Common Language Runtime (CLR) Types. Orion products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance.
- Microsoft SQL Server Native Client
- Microsoft SQL Server Management Objects

Requirements for Virtual Machines and Servers

Orion installations on VMware Virtual Machines and Microsoft Virtual Servers are fully supported if the following minimum configuration requirements are met for

each virtual machine.

Note: SolarWinds strongly recommends that you maintain your SQL Server database on a separate physical server.

Virtual Machine Configuration	IPAM Requirements by License Level		
	IP1000, or IP4000	IP16000	IPLX
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
Allocated Hard Drive Space	2GB	5GB	20GB
	Note: Due to intense I/O requirements, SQL Server should be hosted on a separate physical server configured as RAID 1+0. RAID 5 is not recommended for the SQL Server hard drive.		
Memory	3 GB	4 GB	4 GB
Network Interface	Each virtual machine on which IPAM is installed should have its own, dedicated network interface card. Note: Since Orion uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your Orion server, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.		

Requirements for the Orion Database Server (SQL Server)

The following table lists software and hardware requirements for your Orion database server.

Requirements	IP1000, or IP4000	IP16000	IPLX
SQL Server	SQL Server 2005 SP1 Express, Standard, or Enterprise SQL Server 2008 R2 (without SP, SP1, or SP2) Express, Standard, or Enterprise SQL Server 2012 SP1 Express, Standard, or Enterprise SQL Server 2014 Express, Standard, or Enterprise		

	Notes: • Due to latency effects, SolarWinds does not recommend installing your SQL Server and your IPAM server or additional polling engine in different locations across a WAN. For more information, see SolarWinds Knowledge Base article, "Can I install my Orion server or Additional Polling Engine and my Orion database (SQL Server) in different locations across a WAN?" • Either mixed-mode or SQL authentication must be supported. • If you are managing your Orion database, SolarWinds recommends you install the SQL Server Management Studio component. • If your Orion IPAM product installs SQL Server System CLR Types, a manual restart of the SQL Server service for your Orion database is required. • Use the following database select statement to check your SQL Server version, service pack or release level, and edition: **select SERVERPROPERTY ('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')**		
SQL Server Collation	English with collation setting SQL_Latin1_General_CP1_CI_AS English with collation setting SQL_Latin1_General_CP1_CS_AS German with collation setting German_PhoneBook_CI_AS Japanese with collation setting Japanese_CI_AS Simplified Chinese with collation setting Chinese_PRC_CI_AS		
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz

Hard Drive Space	2 GB	5 GB	20 GB
	Note: Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended the SQL Server database and Orion data and log files. RAID 5 is not recommended for the SQL Server hard drive. The Orion installer needs at least 1GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on drive as your server operating system.		
Memory	2 GB	3 GB	4 GB
	Note: SolarWinds recommends additional RAM, up to 8 GB, for Orion IPAM installations including more than 1000 monitors.		

The Configuration Wizard installs the following required x86 components if they are not found on your Orion database server:

- SQL Server System Common Language Runtime (CLR) Types. Orion products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance.
- Microsoft SQL Server Native Client
- Microsoft SQL Server Management Objects

Upgrade Paths

SolarWinds Orion modules and standalone products are compatible with the specific versions of SolarWinds Orion Network Performance Monitor (NPM). Reference this KB article for the latest.
http://knowledgebase.
SolarWinds
.com/kb/questions/1888/Upgrade+paths+for+
SolarWinds+Orion+product+modules+and+standalone+products

Standalone products do not require any other SolarWinds products to be installed. To upgrade from earlier versions of IPAM, follow the given upgrade path.

Excluding Orion Data Directories from Anti-Virus Scanning

Anti-virus programs may lock files used by the SolarWinds Job Engine v2 during scanning. This can cause the SolarWinds Job Engine v2 services to stop and restart, causing delayed polling and gaps in data for a poll cycle.

Therefore SolarWinds recommends that you exclude the following Orion data directory (depending on your Windows platform) from your anti-virus scanning to improve performance and stability:

- For Windows XP/Server 2003: **c:\Documents and Settings\All Users\Application Data\SolarWinds**
- For Windows Vista/7/Server 2008: **c:\ProgramData\SolarWinds**

IPAM Licensing

IPAM is licensed in accordance with the number of IP addresses you manage in one of three statuses; Used, Reserved and Transient. Unused and available IPs do not count towards managed IP count. The following licensing tiers of IPAM are currently available:

- IPAM IP1000 for managing up to 1024 managed IP addresses.
- IPAM IP4000 for managing up to 4096 managed IP addresses.
- IPAM IP16000 for managing up to 16384 managed IP addresses.
- IPAM IPX for managing an unlimited number of managed IP addresses.

For DHCP & DNS Nodes:

- IP1000 = 1000 Nodes
- IP4000 = 4000 Nodes
- IP16000 = 16000 Nodes
- IPX = Unlimited Nodes

IPAM allows you to designate managed IP addresses for management up to your license limit using any of the following methods:

Note: **SolarWinds does not recommend managing more than 1 million addresses per installation.**

Activating Your License

After installing the software through the setup wizard, you are prompted to enter the license activation key for your product. If you do not have an activation key, the product runs in a time-limited evaluation mode.

To evaluate the software without a license:

Click **Continue Evaluation**.

To license the software on a server with Internet access:

1.Click **Enter Licensing Information**.

2.Select **I have internet access and an activation key**.

3.Click the http://www.SolarWinds.com/customerportal link to access the customer portal on the SolarWinds web site.

4.Log on to the portal using your SolarWinds customer ID and password.

5.Click **License Management** on the left navigation bar.

6.Navigate to your product, choose an activation key from the **Unregistered Licenses** section, and then copy the activation key.

7.***If you cannot find an activation key in the Unregistered Licenses section,*** contact SolarWinds customer support.

8.Return to the Activate window, and then enter the activation key in the **Activation Key** field.

9.***If you access Internet web sites through a proxy server,*** click **I access the internet through a proxy server**, and enter the proxy address and port.

10.Click **Next**.

11.Enter your email address and other registration information, and then click **Next**.

To license the software on a server without Internet access:

1.Click **Enter Licensing Information**

2.Select **This server does not have internet access**, and then click **Next**.

3.Click **Copy Unique Machine ID**.

4.Paste the copied data into a text editor document.

5.Transfer the document to a computer with Internet access.

6.On the computer with Internet access, complete the following steps:

7.Browse to http://www.SolarWinds.com/customerportal/licensemanagement.aspx and then log on to the portal with your SolarWinds customer ID and password.

8.Navigate to your product, and then click **Manually Register License**.

9.If the **Manually Register License** option is not available for your product, contact SolarWinds customer support.

10.Provide the Machine ID from Step 5, and then download your license key file.

11.Transfer the license key file to the server.

12.Return to the Activate IPAM window, browse to the license key file, and then click **Next**.

Maintaining Licenses with License Manager

SolarWinds License Manager is an easily installed, free utility that gives you the ability to migrate Orion licenses from one computer to another without contacting SolarWinds Customer Service. The following sections provide procedures for installing and using License Manager.

Installing License Manager

Install License Manager on the computer from which you are migrating currently licensed products.

Note: You must install License Manager on a computer with the correct time. If the time on the computer is off by as little as 5 minutes, in either direction, from Greenwich Mean Time (GMT), you will be unable to reset licenses without calling SolarWinds Customer Service. Time zone settings do not affect and do not cause this issue.

To install License Manager:

1.Navigate to http://support.SolarWinds.com/support/default.cfm.

2.Provide your SolarWinds Customer ID and password, and then click **Login**.

3.Click **Downloads & Updates** in the left navigation pane.

4.Locate the Download Licensed Software section of the page, and click **SolarWinds License Manager**.

5.Unzip the downloaded file, and then run **LicenseManager.exe**.

Using License Manager

You must run License Manager on the computer where the currently licensed SolarWinds product is installed before you can move licenses to a new installation. The following procedure deactivates currently installed licenses that can then be transferred to a new installation.

Checking License Status

Orion IPAM provides a tool to display the current usage of your license by indicating the number of currently managed addresses. This number also appears in the bottom right of the Manage Subnets page.

1.Click **Start > All Programs > SolarWinds Orion > Orion IP Address Manager > Orion IP Address Manager Licensing**.

2.Click **Restart IPAM Services** to update the website with the license change**.**

3.Click **Close**.

To deactivate currently installed licenses:

1.Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.

2.Check products to deactivate on this computer, and then click **Deactivate**.

3.Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

Note: Deactivated licenses are now available to activate on a new computer.

When you have successfully deactivated your products, log on to the computer on which you want to install your products, and then begin installation. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is then assigned to the new installation.

Chapter 3: Common IPAM tasks

The following chapters provide common scenarios for using IPAM.

- Importing your spreadsheets into IPAM
- Creating Subnets
- Managing DHCP Servers
- IP Address Historical Tracking

Chapter 4: Configuring IPAM

IPAM provides an easily configurable user interface. The following sections detail various configurations in your IPAM installation. Select the appropriate section below:

Subnet Scan Settings	System Settings
Duplicate Subnets	Neighbor Discovery
Scanning Credentials	Adding Users
User Role Delegation	Custom User Roles

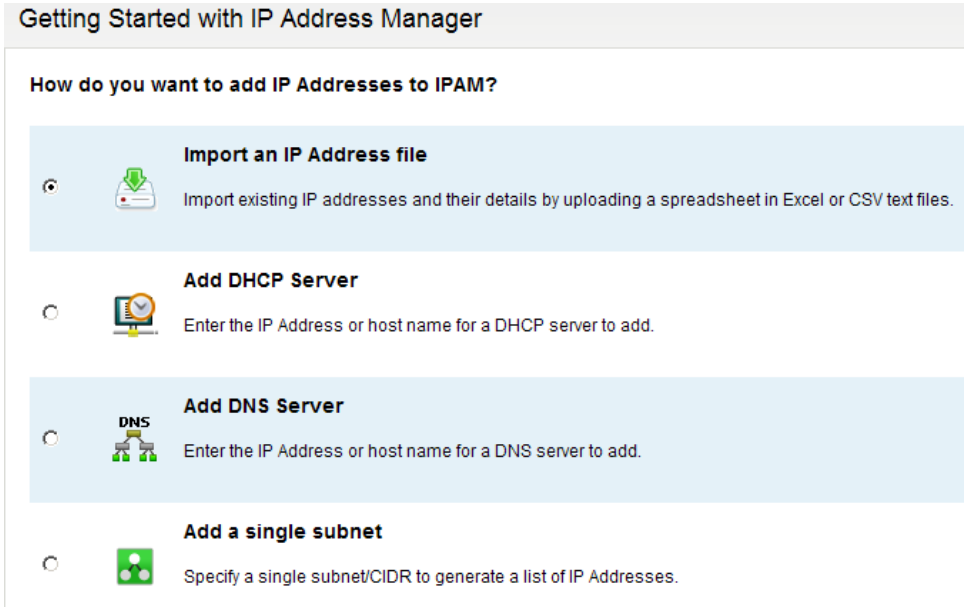
IPAM Getting Started Resource

The **Getting Started with IP Address Manager** resource allows you to quickly begin using Orion IP Address Manager.

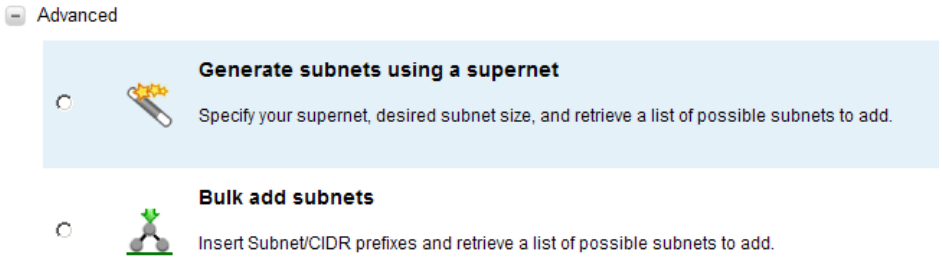
To quickly begin to add Subnets, IP Addresses, DHCP & DNS servers you can you use the Getting Started Wizard.

1.To navigate to the wizard click **Settings > IPAM Settings > Getting Started Wizard.**

2.Select which the appropriate option and click **Start Managing IP Addresses.**



Expand the Advanced Section for more options.



Configuring Subnet Scan Settings

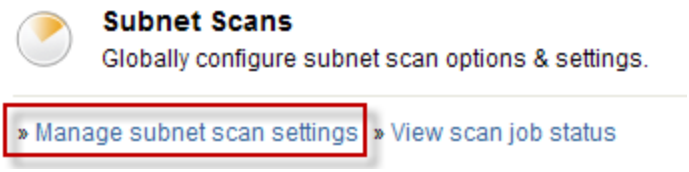
IPAM is capable of using both SNMP and ICMP scanning to continuously determine the status of your monitored network. The Subnet Scan Settings view allows you to select how IPAM automatically scans your network for changes.

To configure Orion IPAM subnet scan settings:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

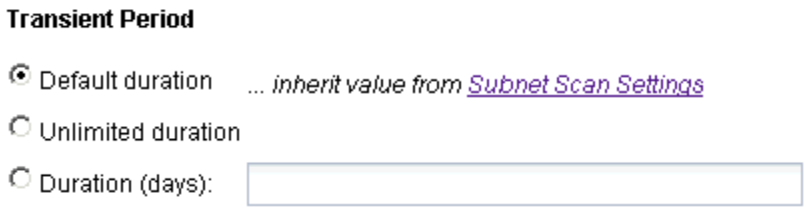
3.Click **Manage Subnet Scans Settings**.



4.Provide an appropriate value for the **Transient Period**. The Transient period must be a value from .2 to 340 days.

IPAM continuously scans all managed IP addresses on your network. If a device fails to respond to any SNMP or ICMP requests for the period of time designated as the **Transient Period**, Orion IPAM changes the status of the unresponsive IP address from **Used** to **Available**. Any associated custom attribute will be overwritten.

You can assign Transient scan intervals on a per subnet basis from the **Edit Subnet** window.



5.Enter the maximum number of simultaneous scans you want IPAM to attempt.

6.***ICMP is used by default to scan your network subnets for changes,*** complete the following steps to configure ICMP:

a.Provide an appropriate number of **Pings per address**.

b.Designate both the **Delay between Pings** and the **Ping Timeout**, in ms, for ICMP requests on your network.

7.***If you want to collect device details using SNMP to scan your network subnets,*** complete the following steps:

a.Check **Enable SNMP Scanning** in the SNMP Scanning section.

b.Provide an appropriate number of **SNMP Retries**.

c.Designate the **SNMP Timeout** for SNMP requests on your network. The timeout value is measured in milliseconds.

d.Enable SNMP neighbor scanning.

8.Click **Save**.

Note: You can disable scanning on a per subnet basis. For more information about editing subnet properties, see “Editing Subnets”.

Credentials

The following sections detail how to configure the credentials needed to manage devices using IPAM. In addition, various user roles can be created to allow for the selected functionality.

- See "Managing Windows Credentials " on page 30
- See "Managing SNMP Credentials " on page 31
- See " Managing CLI Credentials for Cisco DHCP Scope Scans" on page 34
- IPAM User Roles Delegation

Managing Windows Credentials

The Windows Credentials view allows you to configure and save Windows credentials for use when scanning Windows DHCP devices on your network. The following sections provide instructions for managing Windows credentials for your devices.

Adding Windows Credentials

The following procedure helps you store Windows credentials for Orion IPAM. Orion IPAM attempts to communicate with your DHCP network devices using these credentials.

To add a Windows Credential to Orion IPAM:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **Manage Windows Credentials for Scope scans**.

4.Click **Add** in the tool bar.

5.Provide an appropriate **Display Name** for your new credential.

Note: The Windows Credentials view uses the Display Name to reference the different Windows credentials you have saved.

6.Enter the **Password** of your new credential.

7.Click **Save**.

Note: All Windows credentials are sent in clear text during configuration only. Consider updating credentials while locally logged into the IPAM server or over an HTTPS connection. The Windows account specified within IPAM must be on the DHCP server and of the three following groups: DHCP Users, DHCP Administrators and or local Administrators. IPAM impersonates the specified account on the local computer in order 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.

Managing SNMP Credentials

The SNMP Credentials view allows you to configure and save SNMP credentials for use when scanning SNMP devices on your network. The following sections provide instructions for managing SNMP credentials for your devices.

Adding SNMP Credentials

The following procedure helps you store SNMP credentials for Orion IPAM. Orion IPAM attempts to communicate with your network devices using the credentials in the order they are entered. To change the SNMP credential order see Ordering SNMP Credentials .

To add an SNMP credential to Orion IPAM:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **SNMP Credentials**.

4.Click **Add** in the tool bar.

5.Provide an appropriate **Display Name** for your new credential.

Note: The SNMP Credentials view uses the Display Name to reference the different SNMP credentials you have saved.

6.Select the **SNMP Version** of your new credential.

Notes:

- Orion IPAM uses SNMPv2c by default. If the credential you are adding is required to scan devices using the enhanced security features of SNMPv3, select **SNMPv3**
- If you select SNMPv2c and you do not want Orion IPAM to use SNMP v1 if an SNMPv2c request fails, confirm that **Use SNMP v2 only** is checked.

7.***If the default SNMP port for the devices requiring your new credential is not 161,*** provide the actual **SNMP Port** number for these devices.

8.***If you want to use either SNMPv1 or SNMPv2c for subnet scanning with your new SNMP credential,*** provide at least one valid read-only **Community String** for the devices you want to scan with your new credential.

Note: Orion IPAM requires the **public Community String**, at minimum, for subnet scanning.

9.***If you want to use SNMPv3 for subnet scanning with your new SNMP credential,*** you will need the following information:

- SNMPv3 User Name and Context
- SNMPv3 Authentication Method and Password/Key
- SNMPv3 Privacy/Encryption Method and Password/Key

10.Click **Save**.

Ordering SNMP Credentials

The following procedure provides the steps required to reorder stored SNMP credentials. Orion IPAM attempts SNMP communication using the stored credentials in the order provided.

To order SNMP credentials in Orion IPAM:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **SNMP Credentials**.

4.Check the credentials you want to reorder, and then click **Up** or **Down** in the tool bar, as appropriate, to move selected credentials up or down, respectively, in the list of stored credentials.

Editing SNMP Credentials

The following procedure guides you through editing stored SNMP credentials Orion IPAM uses to monitor your network.

To edit an SNMP credential in Orion IPAM:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **SNMP Credentials**.

4.Check the Display Name of the credential you want to edit, and then click **Edit** in the tool bar.

5.***If you want to edit the credential Display Name,*** provide the new **Display Name** for the selected credential in the designated field.

Note: The SNMP Credentials view uses the Display Name to reference the different SNMP credentials you have saved.

6.***If you want to edit the SNMP version of the selected credential,*** select a different **SNMP Version** for the selected credential.

Notes:

- Orion IPAM uses **SNMPv2c** by default.
- ***If you select SNMPv2c and you do not want Orion IPAM to use SNMP v1,*** confirm that **Do not drop down to SNMP v1** is checked.
- ***If the credential you are editing is required to scan devices that require the enhanced security features of SNMPv3,*** confirm that **SNMPv3** is selected.

7.***If you want to provide a different SNMP port number for the selected credential,*** provide the new **SNMP Port** number.

8.***If you want Orion IPAM to use either SNMPv1 or SNMPv2c for subnet scanning with the selected credential,*** provide at least one valid read-only **Community String** for the devices to scan with the selected credential.

Note: Orion IPAM requires the **public** Community String, at minimum, for subnet scanning.

9.***If you want Orion IPAM to use SNMPv3 for subnet scanning with the selected credential,*** provide the following settings:

- SNMPv3 User Name and Context
- SNMPv3 Authentication Method and Password/Key
- SNMPv3 Privacy/Encryption Method and Password/Key

10.Click **Save**.

Deleting SNMP Credentials

Complete the following procedure to delete an SNMP credential from the credential library.

To delete an SNMP credential from Orion IPAM:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **SNMP Credentials**.

4.Check the Display Name of the credential you want to delete, and then click **Delete** in the tool bar.

5.Click **Yes** to confirm that you want to delete the selected credential.

Managing CLI Credentials for Cisco DHCP Scope Scans

IPAM gathers data from CISCO devices using CLI commands and telnet or ssh protocols. Verify that your CISCO DHCP servers have configurable connection types (ssh or telnet), ports (default depends on type), and a user name and password.

The section details the how to provide the CLI Credentials IPAM will use to connect to your devices.

- The username and password used is the same user account you would use to log into the device via CLI to perform system configurations.
- The enable level you select must have privileges to execute **configure terminal** commands as well as be able to configure IP SLA operations. For information on configuring network devices, please see your manufacturer's documentation.

Note: As you change passwords on managed devices, ensure that you also change them in the IPAM credentials list.

To add a Cisco CLI credential

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **Manage Credentials for Scope scans**.

4.Click **Add New** in the tool bar and select Cisco.

5.Provide an appropriate **Display Name** for your new credential.

6.Enter the **User Name** of your new credential.

7.Enter the **Password** of your new credential.

8.Select the Enable Level.

9.Enter the Enable Password.

10.Select the correct protocol.

11.Select the associated port.

12.Click **Save**.

IPAM System Settings

The System settings page allows you to define important IPAM variables.

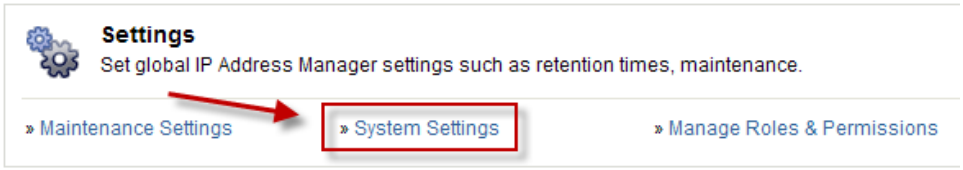
- Enable Duplicate Subnets: When disabled, you cannot create a subnet that is a duplicate or overlaps an existing subnet. The status from multiple DHCP server scopes will merge into one subnet, rather than having different subnets for each server's scope.
- Thresholds: Define the Critical and Warning threshold percentage levels for your IP Address space.
- Configuration Details: Allows you to define if Subnet scans are enabled, default scan intervals, default CIDR value and whether you want IPAM to automatically add IP Addresses.
- Visual Settings: Allows you to define how many items are in the left tree pane, network view items, and IP Address view items.
- Personal Settings: When enabled, this will display a notification message when changes are made to a parent subnet, which contains custom roles.

To edit the IPAM System Settings:

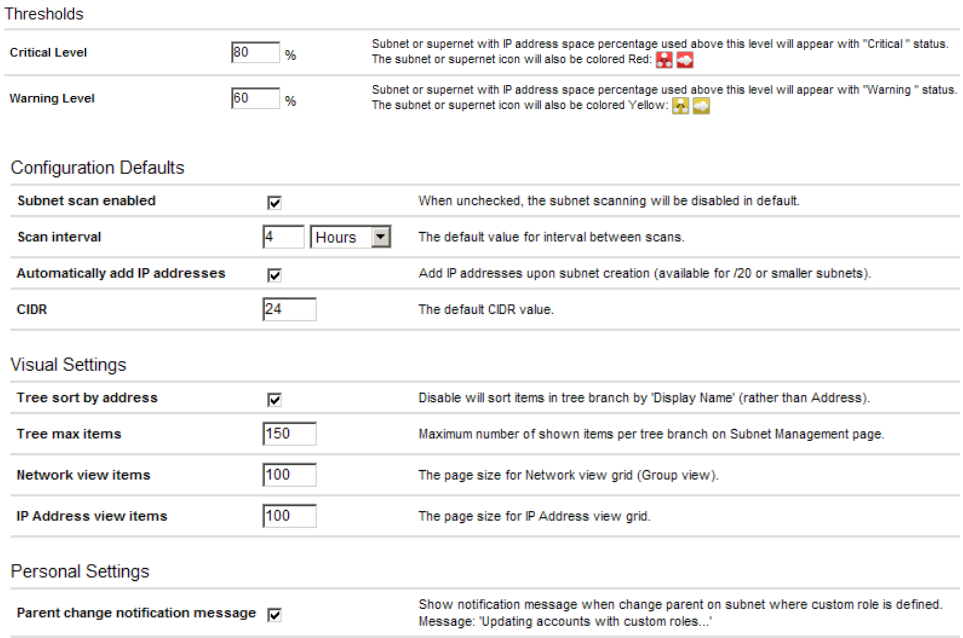
1.Click **Settings** in the upper right corner.

2.Click **IPAM Settings**.

3.Click **System Settings**.



4.Edit as needed (Thresholds, Configuration and Visual settings).



5.Click **Save.**

Allowing Duplicate Subnets

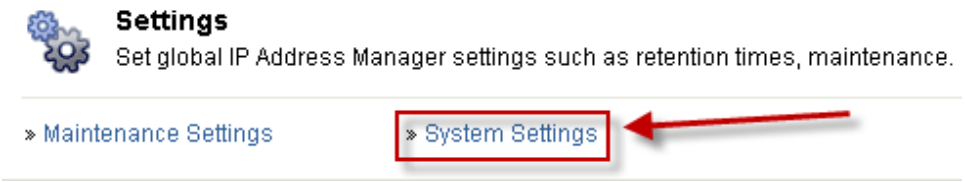
The ability to add duplicate subnets is disabled by default. You can enable this in the IPAM Settings page.

There are some specific use cases where duplicate subnets are desirable. Most of those involve using IPAM as a passive address management system. For

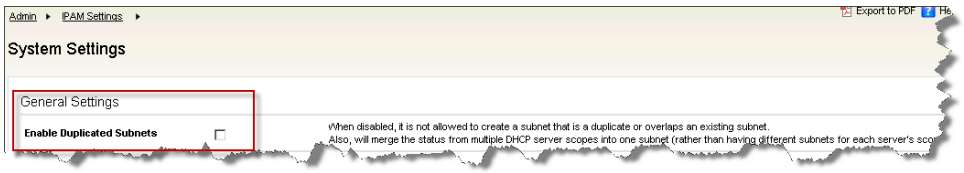
example, if an MSP has customers on duplicate internal addresses, IPAM would allow you to create the duplicate space and give the subnet a different name. Obviously in this scenario, they are not scanning because the scan would return the same results. If you find the need to have duplicate subnets, the following steps detail how to enable this setting.

To enable duplicate subnets:

1.Click **IPAM System Settings.**



2.Check **Enable Duplicated Subnets.**



3.Click **Save.**

Indirect Discovery

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.

Note: Neighbor Scanning is disabled by default.

To enable Neighbor Scanning:

1.From the **Manage Subnets & IP Addresses** tab select a subnet

2.Click Properties

3.Scroll to the bottom of the Subnet Properties window.

4.You should see an option that says "Disable Neighbor Scanning". This is checked (disabled) by default.

5.When you un-check it, additional options will appear where you can add the IP of the neighbor device.

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

- 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.

Creating and Configuring Custom Fields

Depending on the type of component selected, Orion IPAM provides a number of predefined text properties to help organize your network, in addition to the ability to create URL custom links. Users have the ability to add descriptive text fields to addresses, subnets, supernets, and groups or link to external URLs.

Note: The Orion Network Performance Monitor Custom Property Editor capabilities are not integrated with the Orion IPAM module at this time.

To create or edit an Orion IPAM custom field:

1.Click **IP Addresses** in the menu bar.

2.Click **IPAM Settings**.

3.Click **IPAM Custom Fields** > Manage IPAM Custom Fields.

4.***If you want to add a custom field,*** click **Add**.

5.***If you want to edit an existing custom field,*** check the field to edit, and then click **Edit**.

6.Provide a **Database Column** for your custom field. The Database Column is the label used wherever Orion IPAM references the custom field you are defining in the IPAM Web Console.

7.Edit the **Database Column** entry, as appropriate. The value is the alphanumeric label used in the Orion IPAM table of your Orion database for the custom field you are defining. By default, Orion IPAM generates this value sequentially.

8.Edit the **Description** of this field as necessary. The Description text is displayed if the custom field you are defining may be edited.

9.Select the appropriate **Field Type** for the custom property. Text based or a URL linked property.

10.Provide a **Link Title** for your URL link custom property. For example: a link to your IP SLA module web interface.

11.Provide a **Max String Length** for your custom field. The Max String Length sets a limit to the number of characters you may use for any value of the custom field you are defining.

12.***If you want to make this custom field available to all network components defined in Orion IPAM,*** check **Add to Groups, Supernets, and Subnets, DHCP scopes, and DHCP servers**. Making this custom field available to all network components defined within Orion IPAM gives you the option to edit this field whenever you edit any network component.

13.***If you want to make this custom field available to all IP addresses monitored by Orion IPAM,*** check **Add to IP addresses**. Making this custom field available to all IP addresses monitored by Orion IPAM gives you the option to edit this field whenever you edit any IP address.

14.When you have completed configuration of your custom field, click **Save**.

Customizing the IPAM Summary View

The IP Address Manager view provides a highly customizable display of the current status of managed IP addresses on your monitored network. By default, the IP Address Manager view provides the following resources:

- Top 10 Subnets by % IP Address Space Usage
- Top 10 DHCP Scopes by % IP Address Space Usage
- Search for IP Address
- Custom List of Reports
- Getting Started with IPAM Resource
- thwack Recent IPAM Posts

You can customize your IP Address Manager view by adding, deleting, or reordering any available Orion resources.

To customize the IP Address Manager view:

1.Click **IP Addresses** in the menu bar.

2.Click **Customize Page** in the upper right corner.

3.***If you want to change the column layout of your IPAM Summary view,*** click **Edit** and then configure the column layout of your view as follows:

a.Select the number of columns under Layout, and then provide the width, in pixels, of each column in the appropriate fields.

b.***If you have set the column layout for your view,*** click **Submit**.

4.***If you want to add a resource,*** repeat the following steps for each resource that you want to add:

a.Click **+** next to the column in which you want to add a resource.

b.Click **+** next to a resource group on the Add Resources page to expand the resource group tree displaying all available resources for the group.

c.Check the resources you want to add.

d.***If you have completed the addition of resources to the selected view,*** click **Submit**.

5.***If you want to delete a resource from a column,*** select the resource, and then click **X** next to the resource column.

6.***If you want to copy a resource in a column,*** select the resource, and then click  next to the resource column to copy the selected resource.

7.***If you want to change the order in which resources appear in your view,*** select resources, and then use the arrow keys to arrange them.

8.***If you have finished configuring your view,*** click **Preview**.

A preview of your custom view displays in a new window. A message acting as a placeholder may display in some assigned resource locations, and resources will display as empty if resource information has not been polled yet.

9.Close the preview window.

10.***If you still want to change aspects of your view,*** repeat the preceding steps as needed.

11.***If you are satisfied with the configuration of your view,*** click **Done**.

Customize Tab Views

Both the Network View and the IP Address View may be personalized by reordering their respective default column arrangements.

User Role Delegation

As a site administrator, you can use role definitions to restrict user access, as necessary, to maintain security without limiting your ability to delegate required network management activities.

The following section details the following topics:

- Adding User Accounts
- User Role Delegation
- Customizing Roles

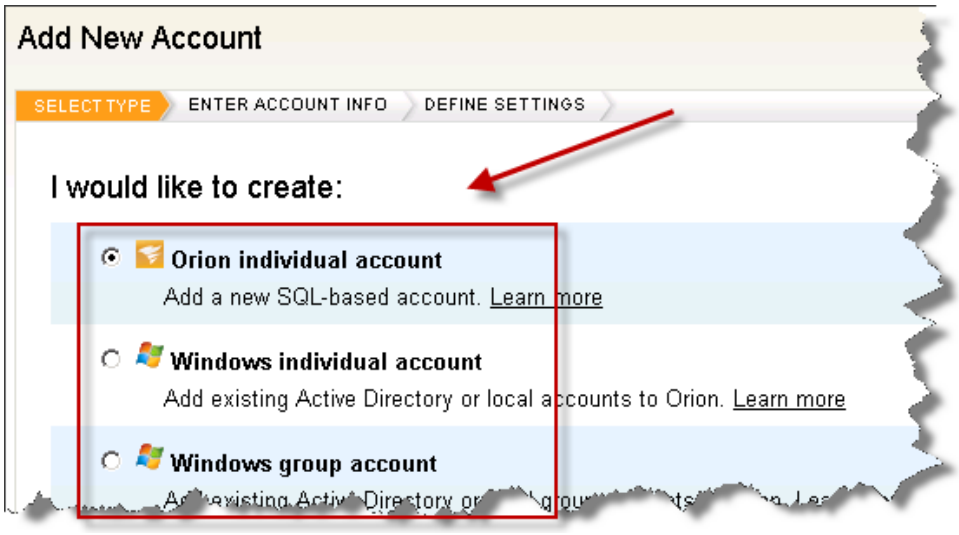
Adding User Accounts

IPAM allows site administrators to securely grant varying privilege levels through user delegation.

To define user roles from the web console menu:

1.Click **Settings > Manage Accounts > Add New Account.**

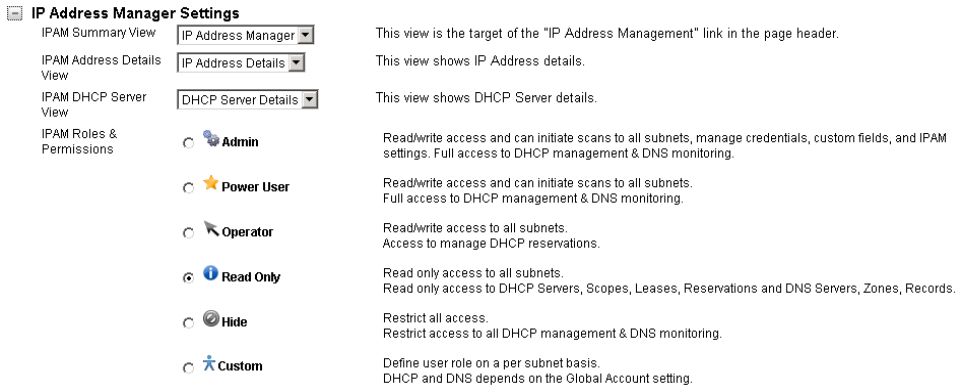
2. Choose which account is applicable and then click **Next**.



3.Enter the credentials and then click **Next**.

4.Define the general settings for Orion, **Account Limitations and Menu Bar views**.

5.Expand the **IP Address Manager Settings.**



For detailed definitions of each role see IPAM User Delegation

As a site administrator, you can use role definitions to restrict user access, as necessary, to maintain security without limiting your ability to delegate required network management activities.

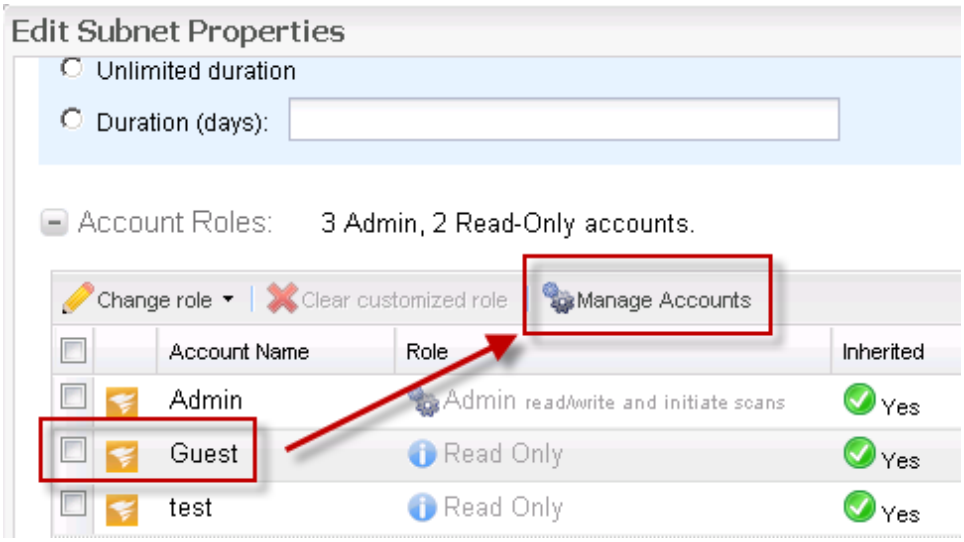
- For example: Defining access roles per subnet, group, or supernet as well as combinations of those containers for specific users

User Role Definitions**".**

If you are defining a custom role see "**IPAM Custom Roles" for more information.***

6.Select the appropriate role and click **Submit.**

Note: Site Administrators can also configure custom roles in the **Edit Subnet** window. Select a subnet > edit > then select Account Roles. Check the **Account** and click **Manage Accounts** to configure.



IPAM User Delegation

As a site administrator, you can use role definitions to restrict user access, as necessary, to maintain security without limiting your ability to delegate required network management activities.

- For example: Defining access roles per subnet, group, or supernet as well as combinations of those containers for specific users

User Role Definitions

The following sections describe user role definitions.

Note: If subnets are moved creating hierarchy changes, inherited roles will be inherited from the new parent. Customized roles will not be changed.

The following user roles are available:

Admin

Read/write access and can initiate scans to all subnets, manage credentials, custom fields, and IPAM settings. Have full access to DHCP management & DNS monitoring.

Administrators are granted the same access to IPAM that is granted to Power Users with the following added privileges:

- SNMP credentials management.
- Custom fields management.
- Subnet scan settings configuration.

- Can directly configure custom roles in the "Subnet Edit" pop-up dialog

 **Power User**

Power Users maintain the same rights granted to Operators with the addition of the following abilities:

- Drag-and-drop reorganization of network components in the left pane of 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 site administrator.

 **Operator**

Operators maintain the same rights granted to Read-Only users with the addition of the following abilities:

- 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 and 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**

Read only access to DHCP Servers, Scopes, Leases, Reservations and DNS Servers, Zones, Records Hide

This role restricts all access, including access to all DHCP Management and DNS Monitoring.

- All IPAM web console resources, including search and Top XX resources not previously limited by Orion account limitations.

- 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 and IP Addresses page.

Hide

- Restrict All access.
- Restrict Access to all DHCP management & DNS Monitoring.

Custom

This role is defined on a per subnet basis. DHCP and DNS access will depend upon the Global account setting for those nodes.

Editing User Roles

The following procedure edits existing IPAM user roles. This is also where you change account passwords.

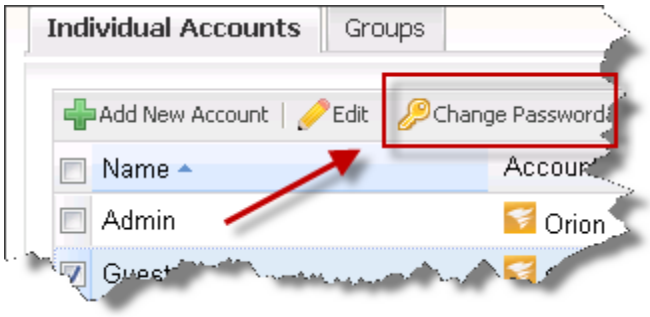
To edit IPAM user roles:

1.Click **Settings > Accounts > Manage Accounts >** in the Views menu bar.

2.Check the Account you wish to edit and click **Edit.**

3.Edit as needed and then click **Submit**.

a.If you need to change the Password, click **Change Password**.



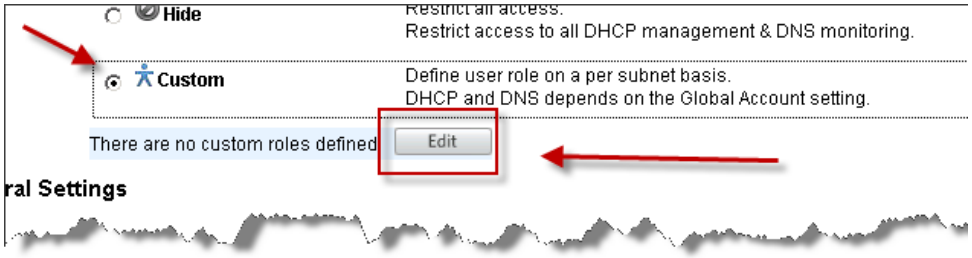
IPAM Custom Roles

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

The visibility of supernets and subnets is affected by 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.

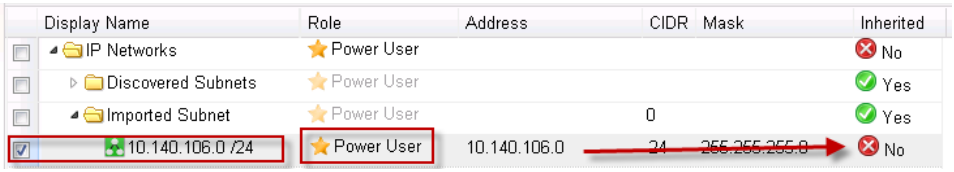
To define a custom role:

1. From the **Role and Permissions** selection box- check **Custom** and then click **Edit**.



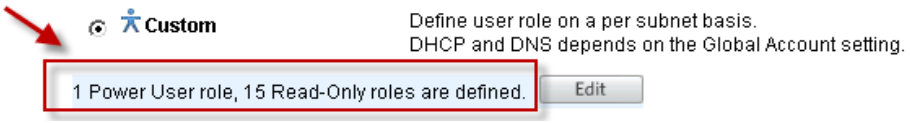
2. Select a group or subnet and then choose a role.

The Inherited Column tells you if the role becomes inherited with other subnets.



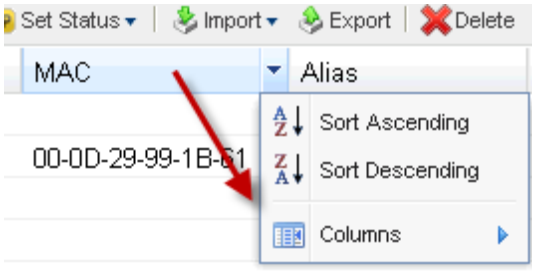
3. You can set permissions for particular subnets by selecting the subnet (check mark) and then selecting a user role. The permission on the child object must be the same or higher than the parent object.

4. After submitting you'll see a confirmation message of the created role.



To customize either the Network View or the IP Address View, simply click a column header and drag it to your preferred location. Your view personalization is

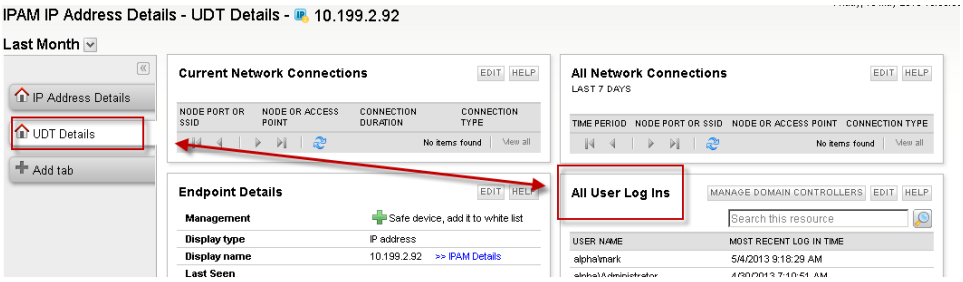
saved immediately, and it is retained for the next time you use Orion IPAM. From the dropdown arrow you can select which resources to add and resize the columns to fit your needs.



User Device Tracker Integration

Integration with User Device Tracker (UDT) adds two columns to your IP Address view providing end-to-end IP address to user/device mapping. The two columns that UDT integration provides are the user and switch ports columns. IPAM detects that UDT is installed and automatically adds the columns.

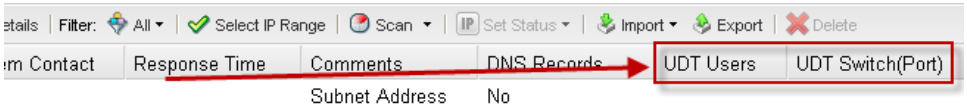
When you click on the IP Address details you will see the UTD Details tab. This tab provides user login and network connection details.



To have data populate the columns, follow the steps below.

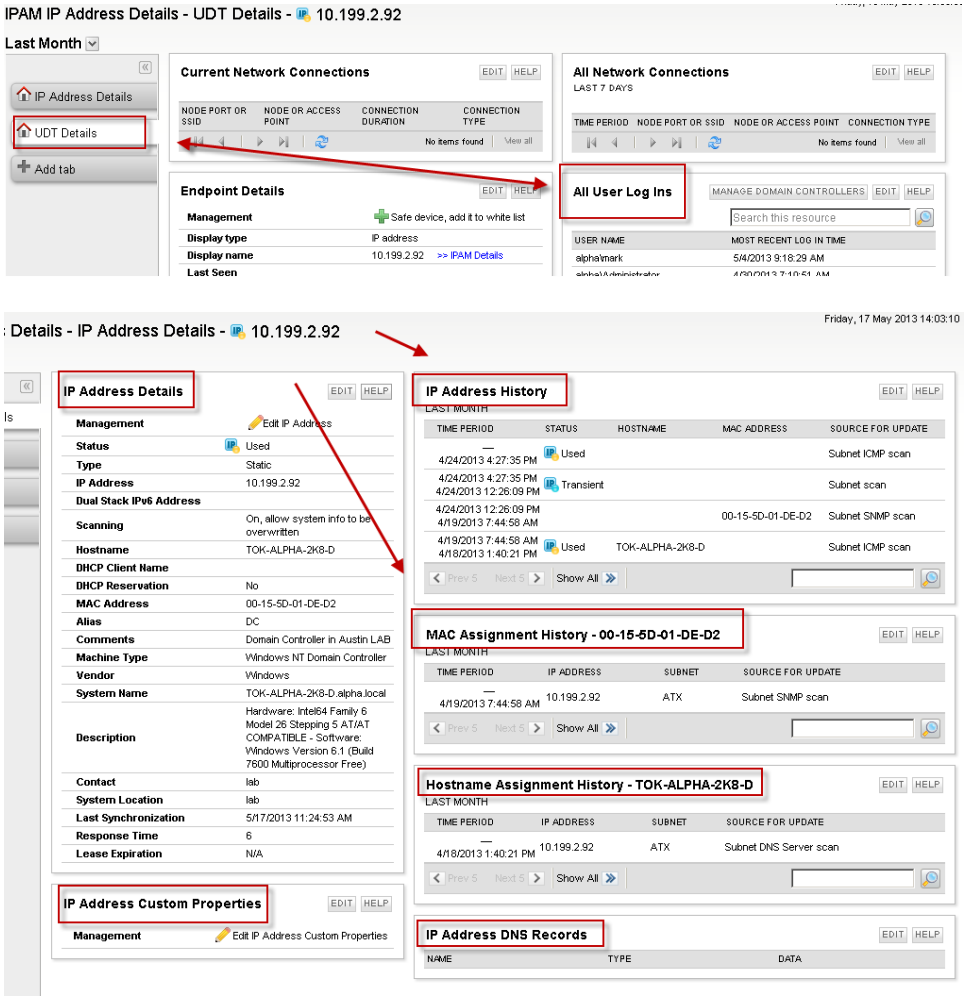
To configure IPAM-UDT integration:

1. Ensure that you have IPAM 3.1.1 installed.
2. Ensure that you have the minimum version of UDT 2.5.0 installed.
3. Login into your web console.
4. Navigate to Manage Subnets & IP Addresses.
5. Two UDT columns will be added to the IP Address view displaying **Users** and **Switch Ports** (scroll far right).



6. In IPAM, add a subnet, for example: (10.199.2.0, 10.199.4.0,10.199.1.0)
7. In UDT add nodes (for example: 10.199.4.1, 10.199.4.5, 10.199.4.11)
8. Add a Domain Controller (AD integrated) in UDT as a node (10.199.1.149, 10.199.1.90) to get the values in Users column
9. Allow for data collection in both IPAM and UDT to begin seeing data in the two columns.

When UDT and IPAM are integrated you will see a UDT Details tab located on the IP Address Details page.



Chapter 5: IP Address Monitoring with IPAM

IPAM automatically monitors all IP addresses in subnets defined with 4096 IP addresses (**/21** or **255.255.248.0** mask) or fewer. These ranges allow you to manage IP addresses in larger subnets.

The following sections provide details about managing IP addresses on your network.

See "DHCP Management" on page 81

See " DNS Management" on page 114

See "Automatic Subnet Discovery " on page 49

Automatic Subnet Discovery

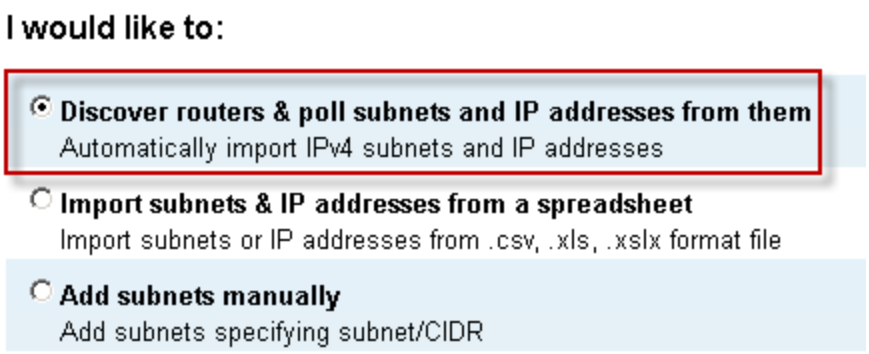
Automatic Subnet Discovery scans selected routers for IPv4 subnets and their IP Addresses and imports them into IPAM.

This automatic process eliminates the need for any manual entry or the importing of IP Address spreadsheets.

In case you want to scan routers that are not monitored nodes simply enter their IP Addresses into the wizard.

Using Automatic Subnet Discovery to Import IP Addresses

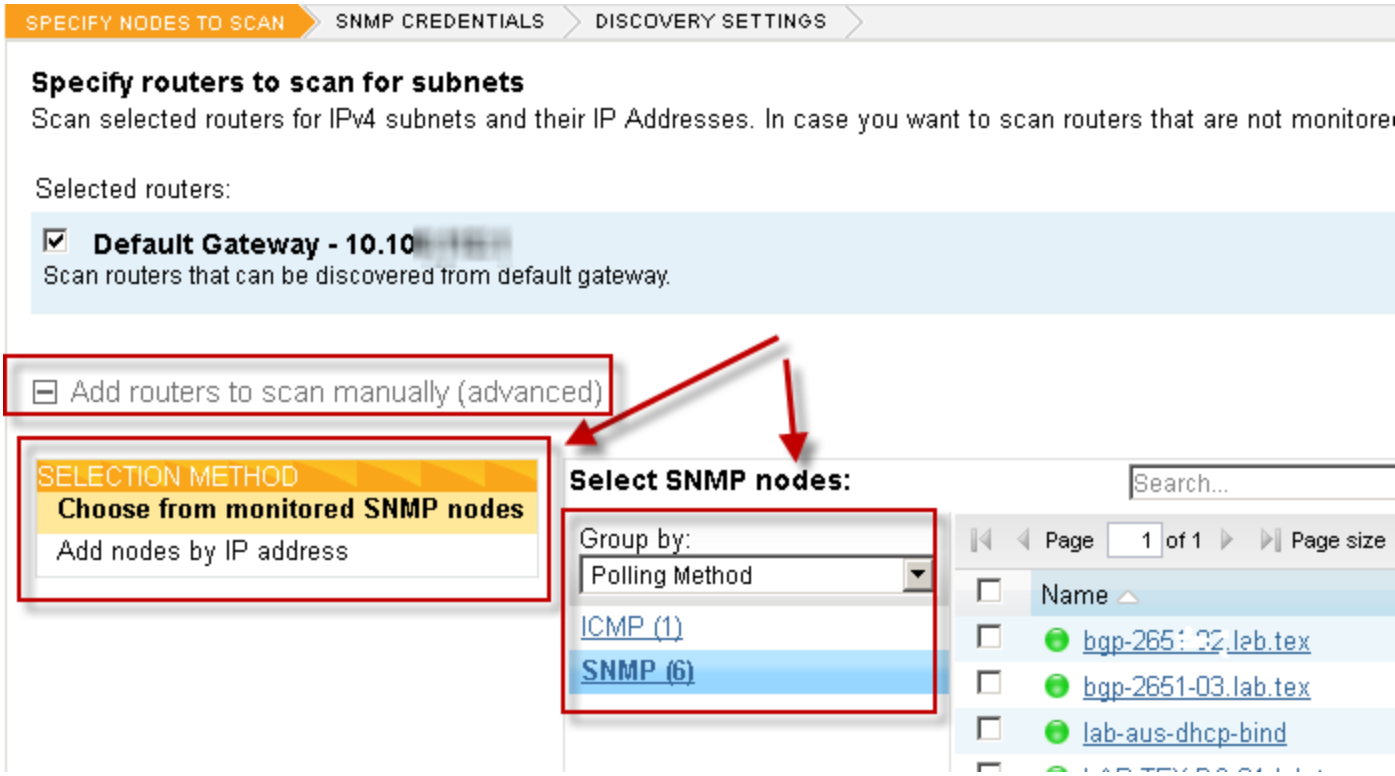
Subnet Discovery is located on the IPAM Settings page and can be accessed from the What's New Resource.



1. Select nodes to scan. You can accept the Default Gateway or manually add routers as needed.
2. Click Add/Edit SNMP Credentials that are used in your network.
3. Adjust the Discovery Settings sliders as needed for Hop Count and SNMP Timeouts.
4. IPAM provides options to organize subnets to existing folders in the Edit screen of subnet results page before importing the discovery results.

Note: IPAM polls the subnets using the devices routing tables.

Images of the Discovery Wizard

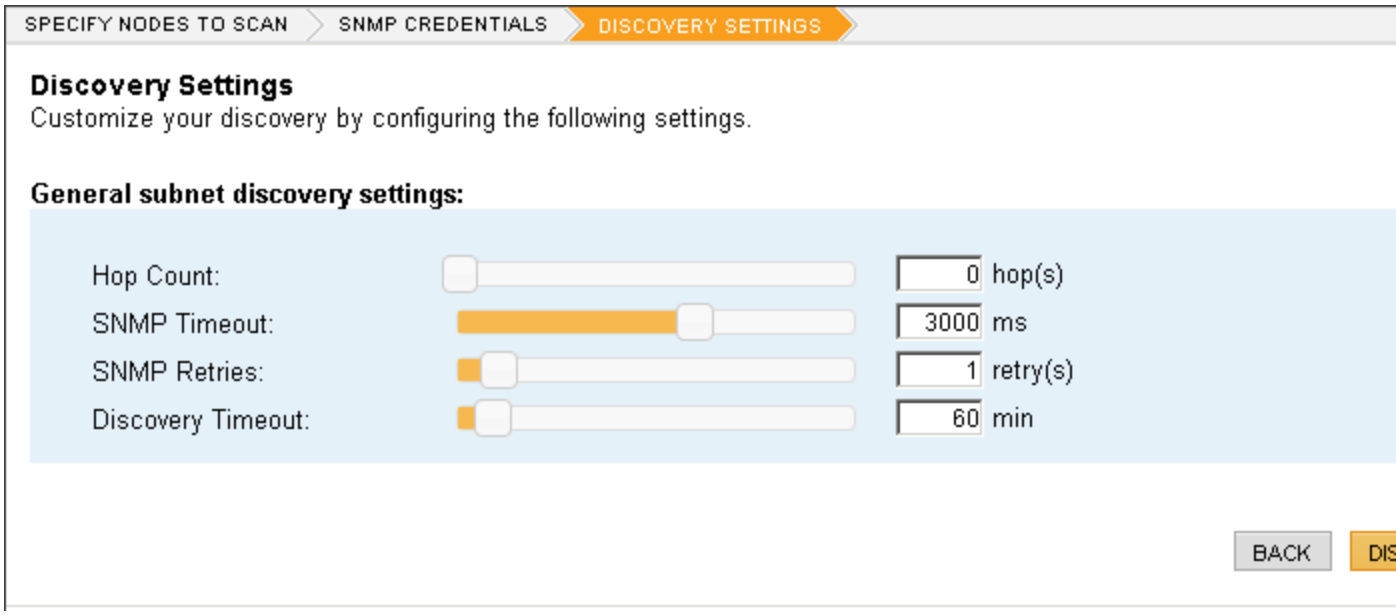


OIDs used during discovery and device polling.

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

How are Hops handled?

IPAM scans the default gateway and any other selected routers within the range of hops you determine.



Adding IP Addresses

The following options are available for adding IP addresses to IPAM:

- Importing your spreadsheets into IPAM
- See "Automatic Subnet Discovery " on page 49
- Manually Add IP Addresses to a Subnet
- Bulk Import Subnets
- Import Addresses into Existing Subnets
- IPV6 Addresses
- IP Address Historical Tracking

    - 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), Orion IPAM automatically monitors all included IP addresses. For more information see Adding IP Address Ranges.

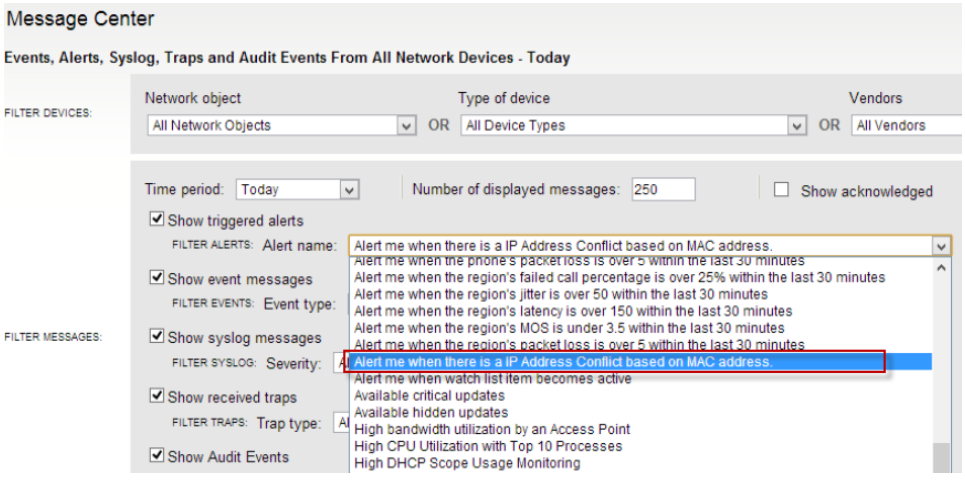
- IP addresses may be added for monitoring by adding a parent subnet into any existing group, supernet, or subnet that Orion IPAM is already monitoring. Adding such a subnet is a straightforward process. For more information about adding subnets, see Creating Subnets.
- The Subnet Allocation Wizard allows you to directly define subnets and allocate included IP addresses.
- IPAM provides the ability to add IPv6 Sites and Addresses for planning purposes. For more information see IPv6 Addresses.

IP Address Conflicts

IPAM actively scans the network and if it detects any duplicate static IP assignments or duplicate IP provisioning from a DHCP server, it will trigger an event. It will also detect if there is more than one MAC address using the same IP Address within the same network.

The event information will display the IP Address, subnet and MAC addresses that are in conflict.

Alerts can be tracked via alert/message center in IPAM. Any alerts/events will appear in the IP Address Summary page – Last XX Events section.



Actively detect IP address conflict. We primarily focused on alerting and information about MAC addresses which is a key-point information for conflict troubleshooting. alert with conflict information:

Once you see IP Address in conflict, simply click on the IP or MAC address info in the alert message and it will take you to the IP address detail view, where you may see MAC address assignment history

So you may directly see device & port where are machines connected with the Universal Device Tracker integration.

Adding a Range of IP Addresses

Particularly in the case of larger subnets, it can be useful to deal with IP addresses in terms of defined IP address ranges, such as **6.6.16.1—6.6.16.15** in a **6.6.16.0 / 20** subnet. The following procedure provides the steps required to add a range of IP addresses within a defined subnet.

Note: By default, IPAM displays all IP addresses in a subnet if the selected subnet contains 4096 or fewer IP addresses (**/21** or **255.255.248.0** and higher mask). For these 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.

To add a range of IP addresses within a defined subnet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**

3.In the network tree pane on the left, click the subnet into which you want to add your new range of IP address range.

Note: For subnets with more than 4096 IP addresses (lower than **/21** or **255.255.248.0** mask), the right pane displays **No IP addresses have previously been added** unless you have already added a range of IP addresses within the selected subnet.

4.Click **IP Range > Add** in the IP Address view in the right pane.

5.Provide both the **Starting IP Address** and the **Ending IP Address** of your new IP address range. Orion IPAM will not allow IP address ranges defined outside the subnet indicated in the Parent Address field.

6.Click **Save**.

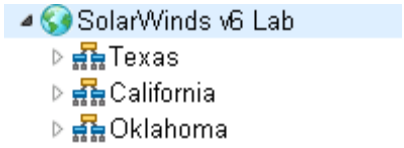
IPv6 Monitoring

Add IPv6 Sites and Subnets to monitor and use the Discover IP address functionality to automatically add existing IPs to subnets.

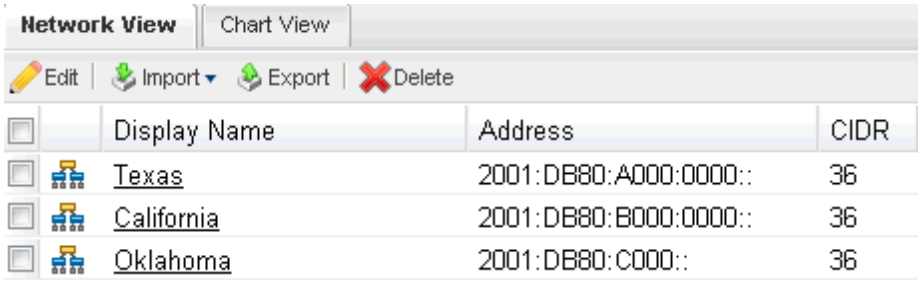
IPv6 addresses can be grouped to assist with network organization. To leverage the amount of addresses available, as well as the organizational features inherent with the implementation, you should create a logical address plan.

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, you would want to designate another nibble for state or location. Finally, you would designate bits for site, building, and floor.

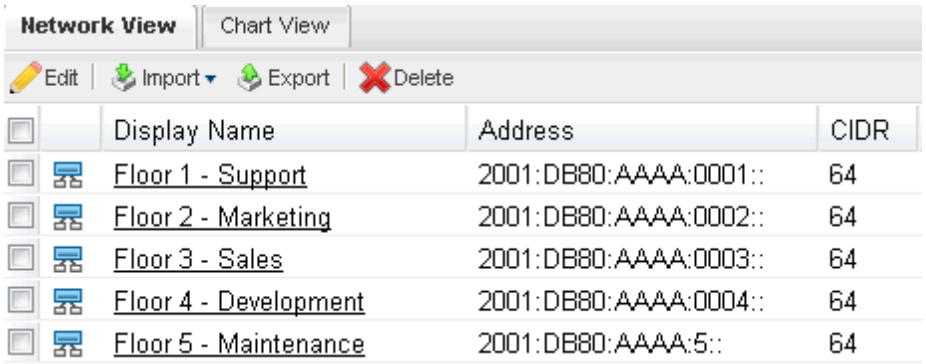
1.Create an IPv6 Global site called SolarWinds v6 Lab.



2.Then add you IPv6 Sites,



3.Then add a building and floors.



IPv6 Scanning

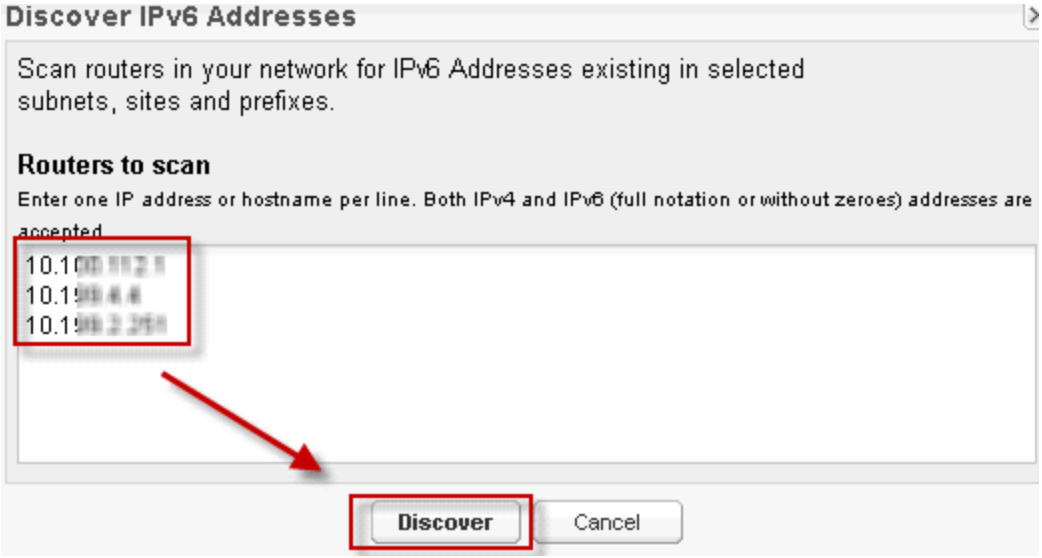
IPAM IPv6 address discovery is based on the NDP protocol and information is obtained from routers based on the following MIBs / OIDs:

- 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)

Note: For troubleshooting purposes verify the device OIDs with those listed above.

You can access this functionality from the IPv6 subnet(s) or IPv6 Global prefix menus by clicking Discover IPs.

Select which routers to scan.



The discovery places all discovered IPs under their respective IPv6 subnet(s) in the selection. All found IPs not belonging to selected subnets are discarded. IPAM uses your existing SNMP credentials to access selected routers.

Adding IPv6 Addresses

The following steps detail the process of adding an IPv6 Addresses. The process entails three parts: Creating an IPv6 Global Prefix, creating an IPv6 Site, and then assigning IPv6 Addresses to the site.

To add an IPv6 Global Prefix:

1.Click **IP Addresses** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.Select a directory folder from the left menu tree and then Click **Add > IPv6 Global Prefix**.*

4.Provide an appropriate **Name** and **Description**.

5. Enter the **Global Prefix address**.

6.Click Save.

*Note: 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 (see RFC 2373 for details). 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:6604:8136:6502::/64 is a possible IPv6 prefix.

Editing an IPv6 Prefix

Once 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, then you can click **Edit** to edit the prefix before adding addresses.

Adding IPv6 Subnets

To add IPv6 subnets:

1.Click IP Addresses in the Menu bar.

2.Click Manage Subnets & IP Addresses.

3.From the left tree menu select the IPv6 Site you want to add the subnet under.

4.Click Add IPv6 Subnet.

5.Enter **Name** and **Description** and click Save.

Adding IPv6 Addresses

To Add IPv6 addresses:

1.Click **IP Addresses** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.Expand the IPv6 Site in the left tree and select the subnet for which you want to assign addresses to.

4.Click Add IP Address.

5.Enter address and select the status as needed and then click Save.

Edit Multiple IPv6 Addresses

To edit multiple IPv6 addresses:

1.Click **IP Addresses** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.Select from the left tree parent IPv6 Subnet.

4.Under the IP Address View tab, place checks in front of the addresses you want to edit. You can select all by checking the top box. Hold down ctrl and click to select various addresses.

5.Click Edit.

6.Click **Save.**

Deleting IP Addresses from Monitoring

Complete the following procedure to delete monitored IP addresses from within a defined subnet.

To delete IP addresses from within a defined subnet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.Click the subnet from which you want to delete a range in the left tree pane of IP addresses.

Note: For subnets with more than 4096 IP addresses (lower than **/21** or **255.255.248.0** mask), the right pane displays **No IP addresses have previously been added** unless you have already added a range of IP addresses within the selected subnet.

4.Check the IP addresses to delete in the right pane IP Address view.

5.Click **IP Range > Remove**.

6.Click **Yes** to confirm the deletion, and then click **Save**.

Setting IP Address Status

The status of any monitored IP address within a defined subnet may be set from the IP Address View on the Manage Subnets and IP Addresses page, as shown in the following procedure.

Note: If a subnet contains more than 4096 IP addresses (lower than **/21** or **255.255.248.0** mask), Orion IPAM only displays IP addresses in previously added ranges. For these larger subnets, you must add IP address ranges for monitoring before Orion IPAM can display addresses that may be managed.

To set the status of an IP address within a defined subnet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**, and then click the subnet containing the IP address for which you want to set the status in the left tree pane.

Note: For subnets with more than 4096 IP addresses (lower than **/21** or **255.255.248.0** mask), the right pane displays **No IP addresses have previously been added** unless you have already added a range of IP addresses within the selected subnet.

3.Check the IP addresses to modify in the right pane IP Address view.

4.Click **Set Status**, and then select the appropriate status. For more information about the definition of available status icons, see “IPAM Status Icons”.

Editing IP Address Properties

IPAM can store a wide array of information about the devices to which IP addresses are assigned. The following table lists the properties IPAM can record in the IPAM table of your Orion database.

IP Address Properties		
Comment	DNS	IPv6 Address
Last Credential	Last Response Time	Last Synchronization
MAC Address	Machine Type	Node Alias
Status	System Contact	System Description
System Location	System Name	Type
Vendor	Device Status	Dynamic
Lease Expiration	Scanning Status	Node Alias

You can edit IP address properties directly from the IP Address View, including custom properties, on the Manage Subnets and IP Addresses page. The following procedure provides the steps required to edit the properties of an IP address within a defined subnet.

Note: If a defined subnet contains more than 4096 IP addresses (lower than **/21** or **255.255.248.0** mask), IPAM only displays IP addresses in previously added ranges. For these larger subnets, you must add IP address ranges for monitoring before IPAM can display addresses that may be managed.

To edit an IP address within a defined subnet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses** tab.

3.Click the subnet containing the IP address you want to edit in the left tree pane.

Note: For subnets with more than 4096 IP addresses (lower than **/21** or **255.255.248.0** mask), the right pane will display **No IP addresses have previously been added** unless you have already added a range of IP addresses within the selected subnet.

4.Check the IP address to edit in the in the right IP Address view pane.

5.Click **Edit** and then select or provide appropriate values for each listed IP address property.

Note: If you have defined custom fields for IP addresses, they are available for editing. For more information about configuring custom fields in Orion IPAM, see "Creating and Configuring Custom Fields".

6.Click **Save** when you have completed configuration of IP address properties.

Note: Selecting the Scanning option to **Off** will not modify values normally overwritten by network scanning.

Multiple Edit IP Address Properties

IPAM allows you to mass edit properties of selected IP Address ranges. Mass editing allows you to change the Status, Type and Scanning statuses for selected ranges, along with additional user fields and system information.

To edit multiple IP ranges:

1.Click **IP Address Manager** in the Menu bar.

2.Click the **Manage Subnets & IP Addresses** tab.

3.Select the subnet you want to edit from the left pane.

4.Click **Select IP Range** from the right menu pane.

5.Enter the starting and ending IP Addresses.

6.Click **Select + Edit** to edit the properties.

7.Check the necessary boxes to edit and select from the dropdown choices.

8.Click Save

Note: System Information will be overwritten if scanning is enabled. You can turn off automatic scanning by selecting **Off** from the **Scanning** dropdown menu.

To remove multiple IP ranges:

1.Click **IP Address Manager** in the Menu bar.

2.Click the **Manage Subnets & IP Addresses** tab.

3.Select the subnet you want to edit from the left pane.

4.Click **Select IP Range**.

5.Enter the starting and ending IP Addresses.

6.Click **Select + Remove** to remove the selected range from IPAM.

7.Click Yes

Searching for IP Addresses

The IPAM Search feature provides the ability to search for all of the IP Address resources existing within the IPAM database. The following table provides the available search criteria.

Search Criteria	Description
All Fields	This field will search all search criteria fields
Alias	Search by the address alias
Comments	Search for a specific comment
Contact	Search for a contact name
DNS	Search using the DNS
Group Description	Search by a group/subnet+ description
Group Name	Search by a group name
Hostname	Search by Hostname
IPv4 Address	Search for a IPv4-formatted addresses
IPv6 Address	Search for a Dual Stack IPv6-addresses
MAC Address	Search by a specific MAC address
Machine Type	Search by the machine type
Scope Name	Search by scope name
Status	Search by status; Used, Available, Reserved, Transient
System Description	Search by system description
System Location	Search by a physical location
System Name	Search by system name
Vendor	Search by vendor

VLAN ID	Search by VLAN ID
Custom Property	Search by an existing custom property

The following procedure details how to use the IPAM search resource.

To search the IPAM table of your Orion database:

1.Click **IP Address Manager** in the Menu bar.

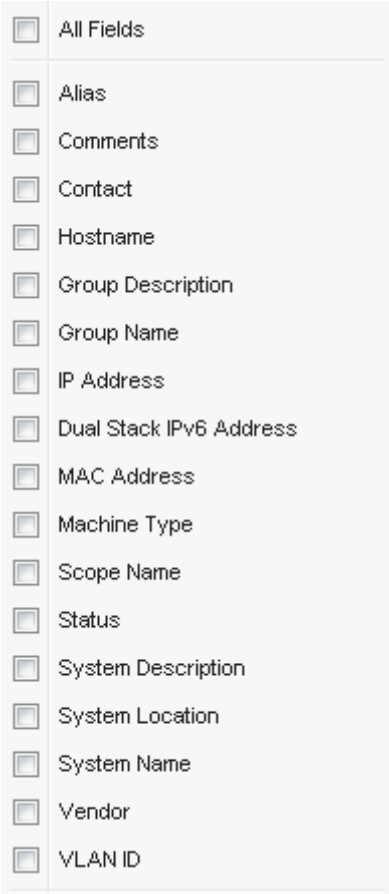
2.Under the Search for IP Address dropdown you can check the criteria relevant to your search.

3.Type a string or IP address and then click **Search**.

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

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

IPAM queries the IPAM table of your Orion database and displays a list of IP addresses matching the provided criteria. Each IP address is listed, in numerical order, with the following user selected information, if available:



Clicking any listed IP address opens the IP Address View for that IP address. From the IP Address View you can edit properties and set the status of the selected IP address. For more information about the IP Address View, see "**Understanding the** IP Address View ".

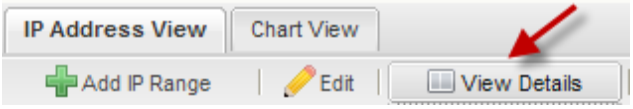
Historical Tracking

IPAM offers the historical tracking of addresses to see how certain properties have changed over time. For example, you can track MAC addresses and hostnames previously assigned to an IP Address.

This feature is available from the IP Address view page by clicking **View Details** and the Search Results page, where you can select the option to include historical results previously assigned to an IP Address.

To view Historical Tracking options from the IP Address view:

1. Select the IP Address you want to view.
2. Click **View Details**.



To view Historical Tracking options using the Search feature:

1.Enter a Search term and proceed to the Search Results page

2.Click **View Assignment History**

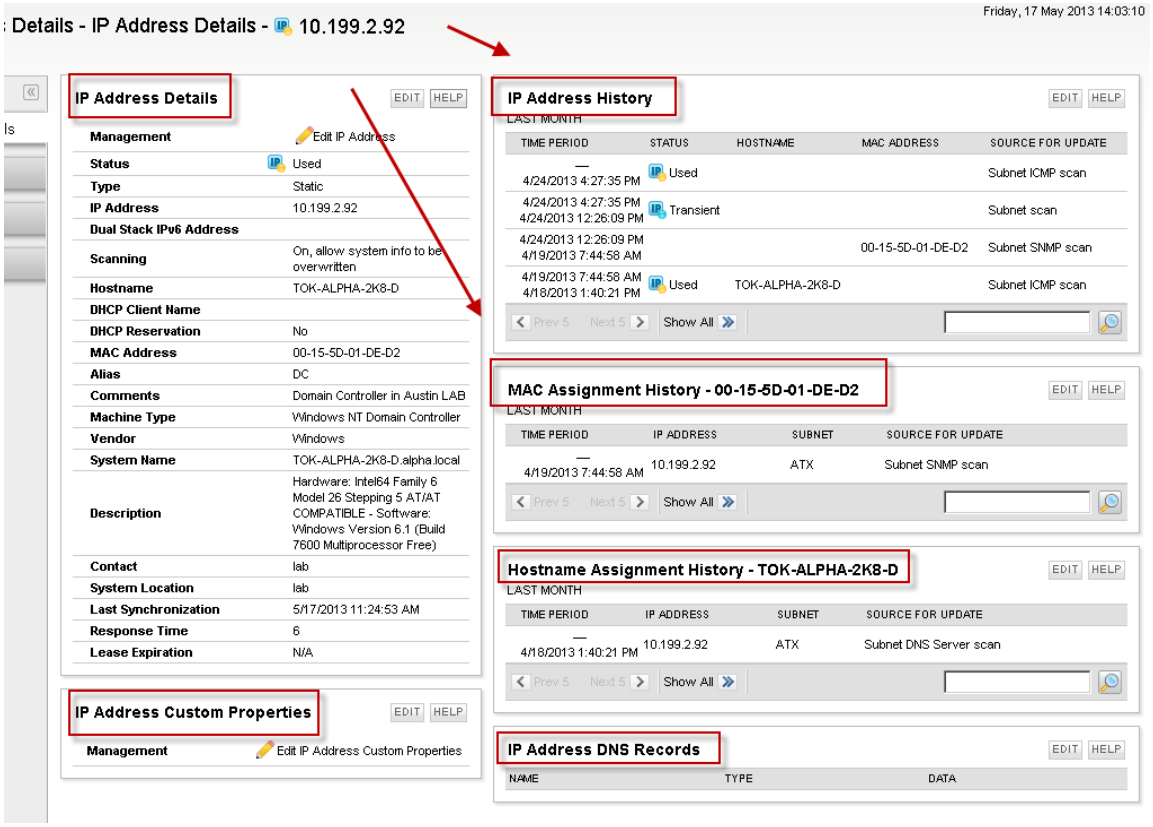
3.Select one of the following: **IP Address Assignment History, MAC Assignment History, and DNS Assignment History**

Note: The displayed DateTime format depends on browser settings, not on regional system settings.

IP Address Details View

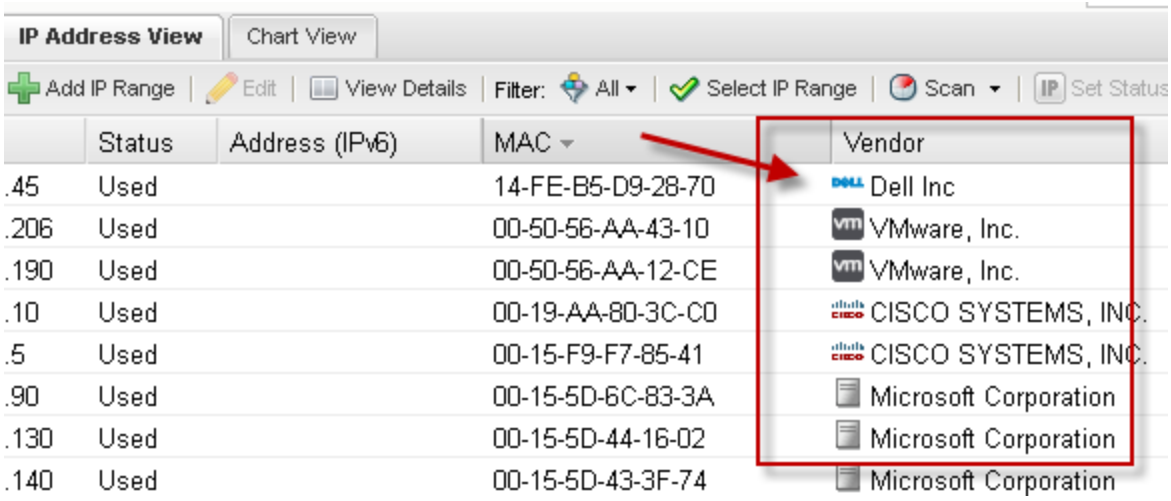
From the IP Address View page you can select a single address and then click **View Details**.

This will display all the details associated with the selected address including Mac /Hostname Assignment history, and DNS Records.



Device Fingerprinting

Vendor icons and Mac Address columns are displayed via the IP Address tab. The vendor identification is based on neighbor scans, SNMP data, and DHCP Leases.

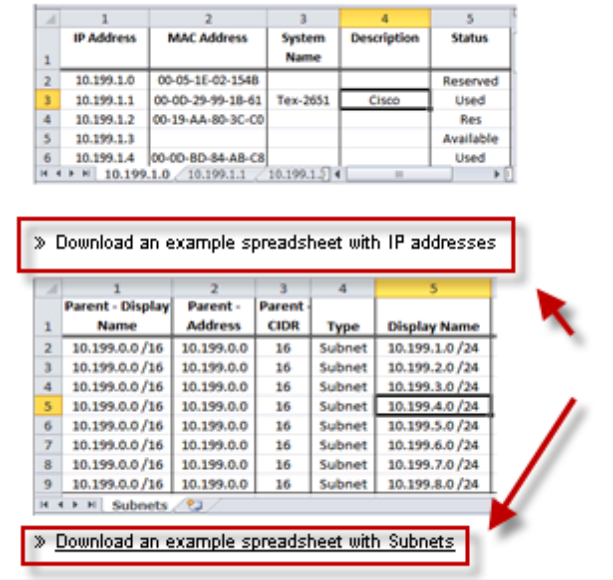


Importing IP Addresses and Subnets

An import wizard will guide you through the process of importing IP Addresses and Subnets. Just follow the onscreen instructions and the wizard will assist with all the required steps.

- Allows user to determine where the IP Address information is imported to.
- The imported data can be distributed in existing IP Addresses across the subnet tree.
- New subnets can automatically be created upon import.
- Can import IP4 & IP6 Groups, Supernets & IPV6 Global prefixes, including subnet tree hierarchy.
- Imported data will respect user delegation permissions.
- The name of the worksheet can have the name of the subnet/CIDR.

Note: Only a .csv, .xls or .xlsx files can be imported. For an example of spreadsheets, click the appropriate example for IP Addresses or Subnets from the links, as seen in the following images.

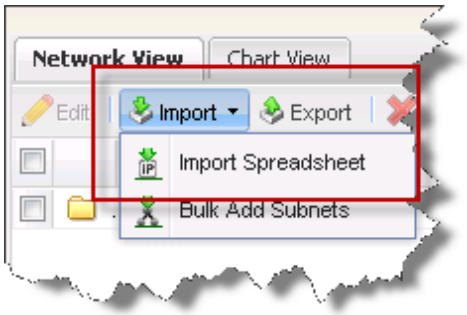


To import IP addresses and settings into IPAM:

If you are importing into existing Addresses see "Importing IP Address into Existing Addresses".

1.Click **IP Address Manager** in the Modules menu bar.

2.Click **Import > Import Spreadsheet**



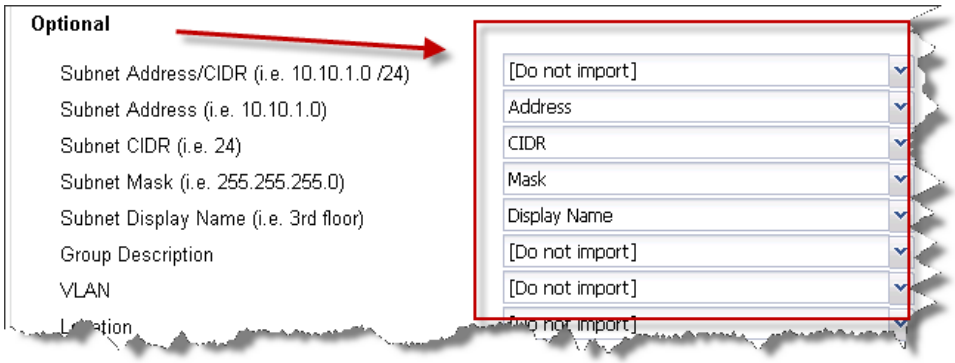
3.Click **Next**

4.Click **Browse**.

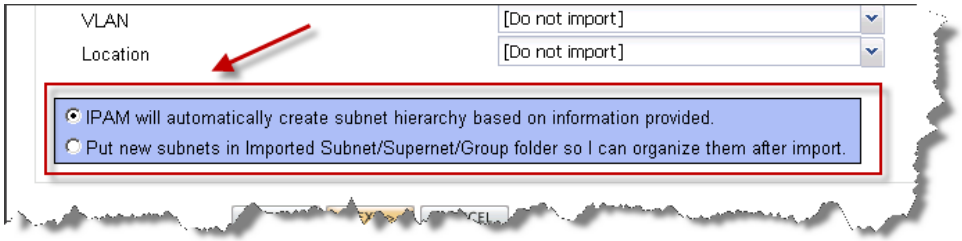
5.Select which content is included in the file import.

6.For each **Database Column** from the import file, select a corresponding **Spreadsheet Column** name to use in the IPAM table of your database and then click **Next**.

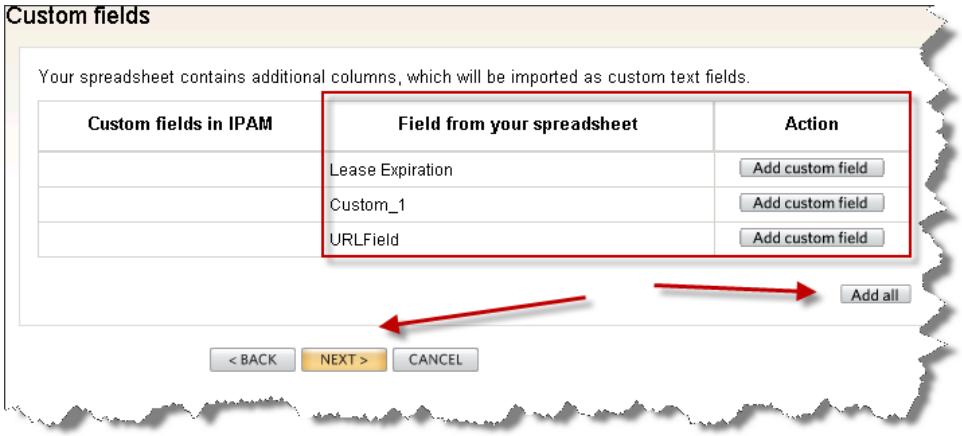
7.Select which optional columns you want to import.



8.Select the option which tells IPAM how to handle the imported content and click **Next**.



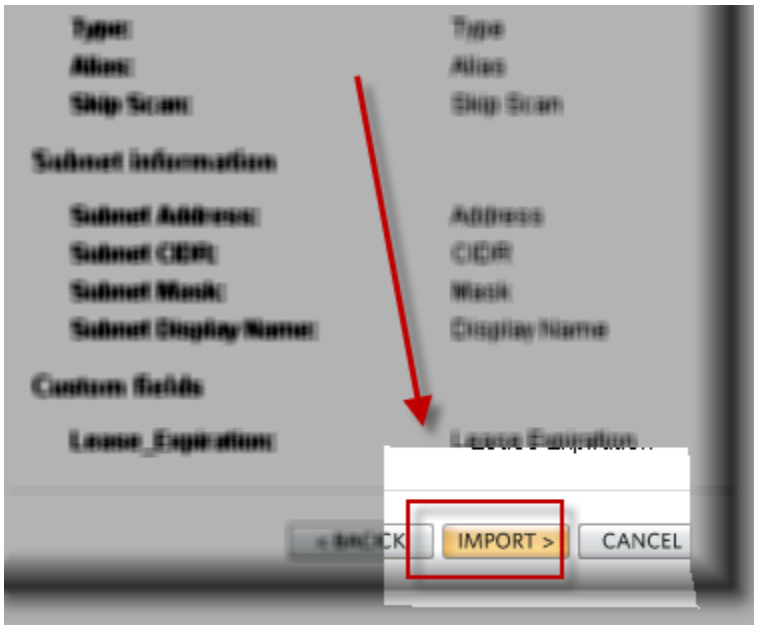
9.If the imported spreadsheet columns contain custom fields, determine which fields you would like to have imported by clicking ***Add custom field.***



a.Click **Save** to add the custom field.

b.Click **Next**.

10.Confirm the selections for import and then click **Confirm**.

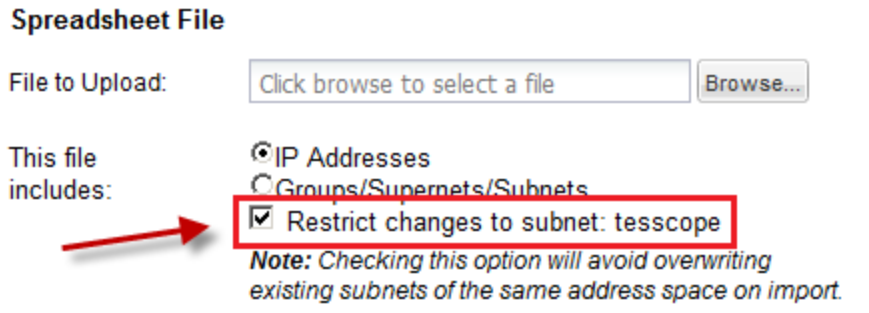


Importing IP Address into Existing Addresses

Select a subnet to import into (open subnet and then click on import), which will be shown on page where you are picking the file. If

Restrict changes to this subnet:

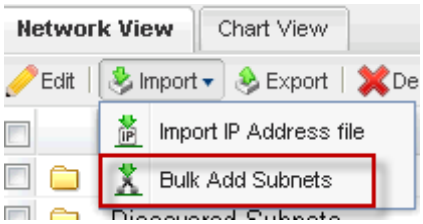
If you restrict changes only to one subnet, other IP addresses outside the subnet range will be ignored, as seen below:



Note: You may see a **Validation Problems** page displayed when there is an issue with the imported file. You can review the information in the grid and also export the errors and correct them in a separate file.

Importing by Bulk Adding Subnets

From the Manage Subnets & IP Addresses page users can easily bulk import subnets by typing or copying IP Addresses in the page.



To import subnets with the bulk feature:

1.Click **Manage Subnets & IP Addresses** tab.

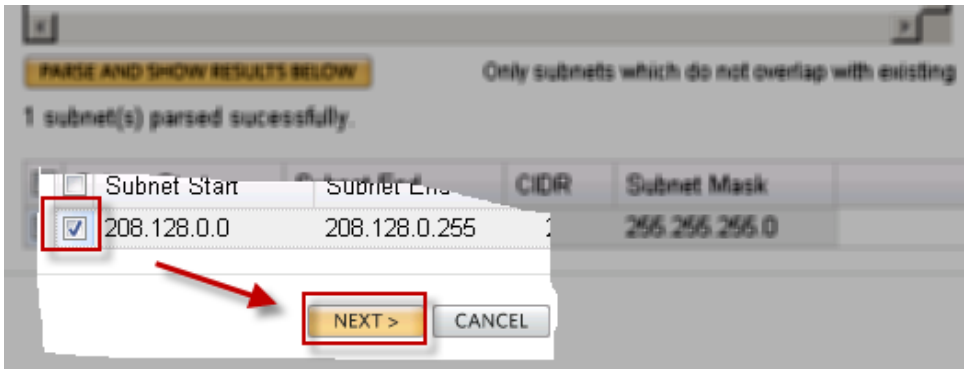
2.Click **Import.**

3.Select **Bulk Add Subnets.**

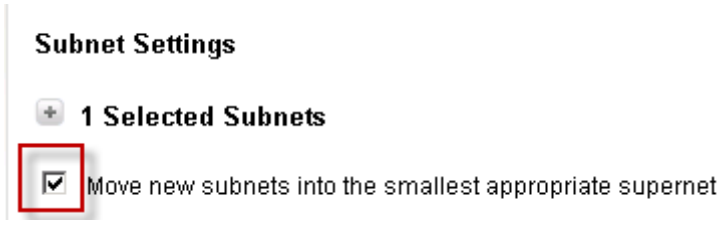
4.Insert Subnet/CIDR Prefixes in the box.

5.Click **Parse and Show Results Below.**

6.Confirm success message and then click **Next.**



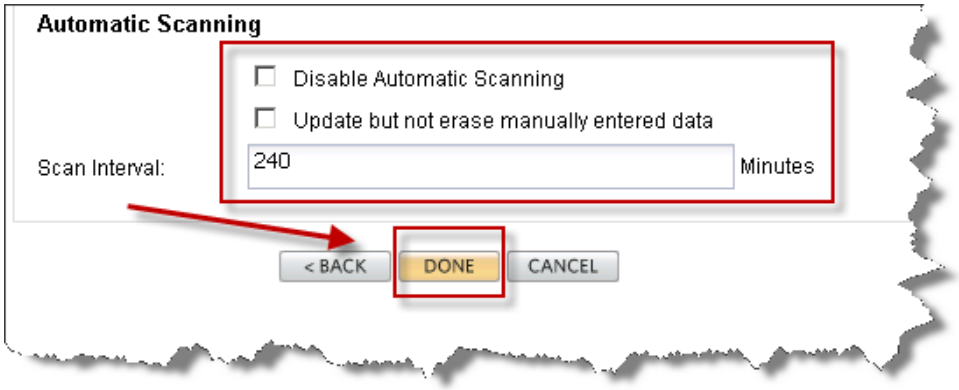
7. ***If you want to move the new subnets into the smallest appropriate supernet*** check **Move new subnets into the smallest appropriate supernet.**



a.Enter appropriate subnet properties.

b.If you do not want system scans to overwrite system information check **Disable Automatic Scanning.**

c.Enter the desired scanning interval in minutes.



8.Click **Done.**

Importing IPs and Subnets from the SolarWinds Engineer's Toolset

To import subnets and IP Addresses from the Engineer's Toolset:

1.Locate the Toolset IP Manager database on your Toolset server.

2.Copy the Toolset IP Address Manager db to an appropriate location on your Orion server.

3.Open a Command Prompt on the Orion server.

4.Enter **CD :\ProgramFiles\SolarWinds\Orion\IPAM**.

5.Enter "**NET STOP "SolarWinds** Orion Module Engine".

6.Enter **SolarWinds.IPAM.Init.exe –import <Fullpath to your Toolset IP Address Manager database>**.

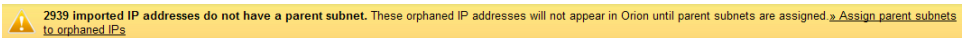
7.Enter **NET START "SolarWinds** Orion Module Engine".

Note: The Toolset IP Address Manager database has an .ipdb extension.

Viewing and Managing Orphaned IP Addresses

After the importing of 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, Orion IPAM requires

that all IP addresses are assigned to a managed subnet, even if the managed subnet contains only a single IP address. If Orion IPAM is unable to locate a configured subnet for each imported IP address, the following warning banner displays above the Manage Subnets and IP Addresses view:



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

Notes:

- If you try to manage more IP addresses than your current license allows, Orion IPAM will add as many IP addresses as allowed. The remaining addresses will be added as orphaned IP addresses.

To assign a parent subnet to an orphaned IP address:

1.Click **Assign parent subnets to orphaned IPs** in the warning banner.

2.Check a single orphaned IP address.

3.Click **Assign Subnet**.

4.***If you do not want to use the default Subnet Name provided by Orion IPAM,*** provide a new **Subnet Name** for the new parent subnet. Orion IPAM suggests both a Subnet Address and a CIDR prefix length based on the actual orphaned IP address. The default Subnet Name provided by Orion IPAM is a concatenation of 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 Orion IPAM,*** provide a new **Subnet Address** and an appropriate **CIDR** prefix length for the new parent subnet.

Notes:

- Orion IPAM suggests both a **Subnet Address** and a **CIDR** prefix length based on the actual orphaned IP address. For more information about CIDR and subnet addressing, see “Networking Concepts and Terminology” on page 3.
- Orion IPAM instantly confirms the validity of provided **Subnet Address** and **CIDR** prefix length combinations. For more information about CIDR and subnet addressing, see “Networking Concepts and Terminology” on page 3.

6.These fields are optional; provide a **Description**, **VLAN ID**, and **Location** for the new parent subnet.

7.Use the slider to set the **Scan Interval**.

8.***If you do not want Orion IPAM to automatically scan your new parent subnet for changes,*** check **Disable Automatic Scanning**.

9.Click **Save** when you have completed configuring your new parent subnet.

Exporting IP Addresses and Settings

Orion IPAM also allows you to export IP addresses and settings, including any custom fields you have defined subnet properties, friendly names, mask, CIDR, as Microsoft Excel (**.xls** and **.csv**) files.

The following procedure exports IP addresses and Subnets from the Orion IPAM table of your Orion database as columns in a new spreadsheet.

To export IP addresses and settings from Orion IPAM:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.***If you want to export an entire group,*** click the parent group of the group you want to export in the network organization pane on the left, and then check the group in the Network View on the right.

4.***If you want to export an entire supernet,*** click a parent group or supernet of the supernet you want to export in the network organization pane on the left, and then check the supernets in the Network View on the right.

Note: Before IPAM can export any supernet, the supernet must be populated with at least one defined subnet.

5.***If you want to export an entire subnet,*** click a parent group or supernet of the subnet you want to export in the network organization pane on the left, and then check the subnets in the Network View on the right.

6.***If you want to export IP addresses,*** click the parent subnet of the IP address you want to export in the network organization pane on the left, and then check the IP addresses to export in the Network View on the right.

7.Click **Export** in the toolbar.

8.Check the columns you want to export.

Note: The IPv4 Address column is selected automatically, and it becomes the first column in the generated spreadsheet. Each additional setting or property you check becomes an additional column in the generated spreadsheet.

9.Click **Export**.

10.When you are prompted to open or save the file, click **Save**.

11.Provide an appropriate file name and location for the generated spreadsheet, and then click **Save**.

Managing Subnets in IPAM

Subnet creation and editing are primary functions of IPAM. The following sections detail the creation and editing of subnets with IPAM.

Creating Subnets

IPAM provides two methods for creating subnets. The IPAM Subnet Allocation Wizard creates subnets within a designated supernet based on a desired subnet size.

For more information about the Subnet Allocation Wizard, see “Using the Subnet Allocation Wizard”.

The second method creates individual subnets within selected subnets, supernets, and groups, directly from the Manage Subnets and IP Addresses page, as shown in the following procedure.

To create a new network subnet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.In the network tree pane on the left, click the network, group, or supernet into which you want to add your new subnet.

4.Click **Add > Subnet**.

5.Provide an appropriate **Subnet Name** for your new subnet. If you leave this field empty, IPAM automatically generates a name based on the **Subnet Address** and **CIDR** prefix length you provide.

6.Provide a new **Subnet Address** and an appropriate **CIDR** prefix length for the new subnet.

Note: IPAM instantly confirms the validity of provided **Subnet Address** and **CIDR** prefix length combinations. For more information about CIDR and subnet addressing, see "Networking Concepts and Terminology".

7.***If you want to further identify your new subnet,*** provide a **Description**, **VLAN ID**, or **Location** for the new subnet.

8.***If you have defined custom fields for subnets,*** provide appropriate values. For more information about configuring custom fields in Orion IPAM, see "Creating and Configuring Custom Fields".

9.Use the slider to set the **Scan Interval**.

10.***If you do not want Orion IPAM to automatically scan your new subnet for changes,*** check **Disable Automatic Scanning**.

11.Click **Save** when you have completed configuring your new subnet.

You can now drag-and-drop your new subnet into other groups and supernets, to organize your network.

Editing Subnets

The edit subnet properties box allows you to edit the properties of an existing subnet, as well as add additional custom information and custom URLs. You can disable the Automatic Scanning or change the scan interval.

To edit an existing network subnet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.Click the subnet you want to edit in the left tree pane.

4.Click **Properties**.

5.Edit the existing **Subnet Name** and the **CIDR** prefix length for your subnet.

6.Edit the **Description**, **VLAN ID**, or **Location** for your subnet, as necessary.

7.Click **Save** when you have completed configuring your subnet.

Managing Subnet Scans

Orion IPAM is capable of conducting both automatic and manual scans of monitored subnets, and the Subnet Scan Status view displays all subnet scans that are either currently in progress or scheduled for completion. Subnet scans are listed according to the Database Column property for each scanned subnet.

For more information about subnet properties, see “Editing Subnets”. For each subnet scan listed, the Subnet Scan Status view displays the following:

- **Status** provides the time when the next scan of the corresponding subnet will begin. If the scan is in progress, Status displays the time elapsed since the scan started.
- The **Scan Type** is either **Automated** or
- **Last Discovery** indicates the date and time when the corresponding subnet was last scanned.

The following procedure provides the steps required to manage subnet scans from the Subnet Scan Status view.

To manage subnet scans:

1.Click **IP Address Manager** in the Menu bar.

2.Click **IPAM Settings**.

3.Click **View subnet scan status** in the Subnet Scans grouping.

4.***If you want to change the settings of any listed subnet scan,*** click **Edit** at the end of the corresponding row.

Clicking **Edit** at the end of a listed subnet scan row opens the Edit Subnet Properties window wherein you can enable or disable automatic scanning and set an appropriate scan interval for the selected subnet. For more information about editing subnet properties, see “Editing Subnets”.

Using the Subnet Allocation Wizard

Orion IPAM provides the Subnet Allocation Wizard to help you efficiently organize your managed IP address space into subnets that are sized appropriately for the extent and traffic of your network. With its real-time subnet calculator, the Orion IPAM Subnet Allocation Wizard allows you to quickly determine the most efficient way to subdivide any supernet, as shown in the following procedure.

To create subnets from supernets using the Subnet Allocation Wizard:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.In the network tree pane on the left, click **Add > Subnet Allocation Wizard**.

4.Type the address of the supernet to divide in the **Supernet Address** field.

5.Select an appropriate **CIDR** prefix length.

Note: Orion IPAM instantly confirms the validity of provided the **Supernet Address** and **CIDR** prefix length combinations. For more information about CIDR, see "Networking Concepts and Terminology".

6.Select the **Desired Subnet Size**.

Note: Typically, in subnets defined to contain more than 2 IP addresses, the first and last addresses are reserved as the network address, for identifying the subnet to the rest of the network, and the broadcast address, for communicating with all addresses within the subnet, respectively. As a result, the number of available IP addresses is always two fewer than the number actually contained within a given subnet.

7.***If you only want to see subnets that have already been allocated,*** clear **Show subnets not already allocated**.

8.Click **Refresh** to display a list of all possible subnets that may be allocated, based on your provided criteria.

9.Check the subnets you want to manage in Orion IPAM, and then click **Next**.

10.***If you want to view the subnets you are currently adding,*** click **+** next to the XX **Selected Subnets** header.

11.***If you do not want to keep the supernet you used on the previous view to define the subnets you are adding,*** clear **Add Supernet** 'X.X.X.X / X'.

Note: By default, Orion IPAM adds the supernet you used to define your subnets to make it easier to organize your network. Although it is optional, SolarWinds recommends that you check this option and use the supernet unless you are only adding a few subnets.

12.***If you do not want to organize your added subnets into the smallest available supernet,*** clear **Move newly added subnets into smallest appropriate supernet**.

Note: Adding subnets either to an existing supernet or to a newly defined supernet can make it easier to organize your network. Although it is optional, SolarWinds recommends that you check this option and keep the supernet unless you are only adding a few subnets.

13.***If you want to further identify your new subnets,*** provide a **Description**, **VLAN ID**, or **Location** for the new subnets.

14.***If you do not want Orion IPAM to automatically scan your new subnets for changes,*** check **Disable Automatic Scanning**.

15.***If you want Orion IPAM to automatically scan your new subnets for changes,*** use the slider to set the **Scan Interval**.

16.Click **Done** when you have completed configuring your new subnets.

Managing Supernets in IPAM

Supernets are extremely useful organizational tools for managing your network. The following sections detail the creation and editing of supernets in Orion IPAM.

Creating Supernets

The following procedure creates a new supernet for organizing your network components.

To create a new network supernet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.In the network tree pane on the left, click the network, supernet, or group into which you want to add your new supernet.

4.Click **Add > Supernet**.

5.Provide an appropriate **Supernet Name** for your new subnet.

Note: If you leave this field empty, Orion IPAM automatically generates a name based on the **Supernet Address** and **CIDR** prefix length you provide.

6.Provide a new **Supernet Address** and an appropriate **CIDR** prefix length for the new subnet.

Note: Orion IPAM instantly confirms the validity of provided **Supernet Address** and **CIDR** prefix length combinations. For more information about CIDR and supernet addressing, see “Networking Concepts and Terminology”

7.***If you want to further identify your new supernet,*** provide a **Description** for the new supernet.

8.***If you have already defined any custom fields for supernets,*** provide appropriate values in the available custom fields. For more information about configuring custom fields in Orion IPAM, see “Creating and Configuring Custom Fields”.

9.When you have completed configuring your new supernet, click **Save**.

You can now drag-and-drop your new supernet into other groups and supernets and drag-and-drop other supernets and subnets into your new supernet to organize your network.

Editing Supernets

The following procedure edits the properties of an existing supernet.

To edit an existing network supernet:

1.Click **IP Address Manager** in the Menu bar.

2.Click **Manage Subnets & IP Addresses**.

3.Click the supernet you want to edit in the left tree pane.

4.Click **Properties**.

5.Edit the existing **Supernet Name** and the **CIDR** prefix length for your supernet.

Note: Orion IPAM instantly confirms the validity of provided **Supernet Address** and **CIDR** prefix length combinations. For more information about CIDR and supernet addressing, see “Networking Concepts and Terminology”.

6.Edit the **Description** for your subnet, as necessary.

7.***If you have defined custom fields for supernets,*** edit the values in the available custom fields, as necessary. For more information about configuring custom fields in Orion IPAM, see “Creating and Configuring Custom Fields”.

8.When you have completed configuring your supernet, click **Save**.

Chapter 6: DHCP Management

IPAM allows you to manage ISC & Cisco DHCP Servers, ASA devices, and Windows DHCP servers.

Choose from the topics below:
Adding DHCP Servers to IPAM (DHCP servers already exist as nodes)
Manually add nodes or add multiple nodes using Discovery Central
DHCP Scopes Management
DHCP Split Scopes
Cisco DHCP & ASA Requirements
ISC DHCP Requirements

Note: Requirements for Monitoring Cisco DHCP servers

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

1.Cisco Commands that need to be supported:
- 'show running-config' - 'show ip dhcp pool' - 'show ip dhcp binding'

a.ASA Devices require these commands:
-show dhcpd binding-show running-config dhcpd-show dhscpd statistics

-show interface l inc interface l ip address

2.The device needs to be a Layer 3 Switch or Router.

3.The IOS must be version 12.2(8)T or later.

4.Enable level 15 is required to view the complete configuration. This is due to how IOS manages permission levels and configuration information. For more

information see http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800949d5.shtml.

ISC DHCP Server Requirements

The following ISC DHCP minimum requirements and configurations are needed for IPAM to access your ISC servers.

-Supported base version for ISC = isc-dhcp-4.2.4-P1

-For more information reference: https://kb.isc.org/article/AA-00736

»Supported Operating System:

-POSIX compliant Linux distributions

»User access:

-User account needs to be configured to allow remote telnet or SSH access to ISC DHCP machine

-Read and write file access for user on the configuration files.

»Cli commands:

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

Note: IPAM will need to seek the config file in one of the following paths below:

»Configuration File:

"/etc/dhcpd.conf"

"/etc/inet/dhcpd4.conf"

"/etc/dhcp/dhcpd.conf"

"/usr/local/etc/dhcpd.conf"

»Lease File:

"/var/db/dhcpd.leases”

"/var/lib/dhcpd/dhcpd.leases"

"/var/lib/dhcp/dhcpd.leases"

"/var/db/dhcpd/dhcpd.leases"

»Script File:

"/etc/init.d/dhcpd"

"/etc/init.d/dhcp"

"/etc/rc.d/dhcpd "

"/etc/init.d/isc-dhcp-server"

"/usr/local/etc/rc.d/isc-dhcpd“

Configuring your ISC DHCP Server:

Note: Nested Configurations are Unsupported.

On the fresh Installation of ISC DHCP from a terminal prompt, enter the following command to install dhcpd: sudo apt-get install isc-dhcp-server

To change the default configuration by editing /etc/dhcp3/dhcpd.conf to suit your needs and particular configuration.

You may also want to edit /etc/default/isc-dhcp-server to specify the interfaces dhcpd should listen to.

By default it listens to eth0.

Next, you would need to assign a static ip to the interface that you will use for dhcp.

Note: Ensure the ISC service is running so IPAM can communicate with your ISC DHCP server. After editing the configuration file, restart the service.

For detailed instructions on configuring your ISC server see the following helpful links:

http://askubuntu.com/questions/140126/how-do-i-configure-a-dhcp-server

https://wiki.debian.org/DHCP_Server

ISC DHCP

Support for ISC DHCP management and monitoring allows you to create, edit, or remove DHCP subnets directly and update servers automatically via the IPAM web interface. 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.

Note: Nested Configurations are Unsupported. For more information see the following KB article.

The following ISC DHCP minimum requirements and configurations are needed for IPAM to access your ISC servers.

-Supported base version for ISC = isc-dhcp-4.2.4-P1

-For more information reference: https://kb.isc.org/article/AA-00736

»Supported Operating System:

-POSIX compliant Linux distributions

»User access:

-User account needs to be configured to allow remote telnet or SSH access to ISC DHCP machine

-Read and write file access for user on the configuration files.

»Cli commands:

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

Note: IPAM will need to seek the config file in one of the following paths below:

»Configuration File:

"/etc/dhcpd.conf"

"/etc/inet/dhcpd4.conf"

"/etc/dhcp/dhcpd.conf"

"/usr/local/etc/dhcpd.conf"

»Lease File:

"/var/db/dhcpd.leases”

"/var/lib/dhcpd/dhcpd.leases"

"/var/lib/dhcp/dhcpd.leases"

"/var/db/dhcpd/dhcpd.leases"

»Script File:

"/etc/init.d/dhcpd"

"/etc/init.d/dhcp"

"/etc/rc.d/dhcpd "

"/etc/init.d/isc-dhcp-server"

"/usr/local/etc/rc.d/isc-dhcpd“

Configuring your ISC DHCP Server:

On the fresh Installation of ISC DHCP from a terminal prompt, enter the following command to install dhcpd: **sudo apt-get install isc-dhcp-server**

To change the default configuration by editing **/etc/dhcp3/dhcpd.conf** to suit your needs and particular configuration.

You may also want to edit **/etc/default/isc-dhcp-server** to specify the interfaces dhcpd should listen to.

By default it listens to **eth0**.

Next, you would need to assign a static ip to the interface that you will use for dhcp.

Note: Ensure the ISC service is running so IPAM can communicate with your ISC DHCP server. After editing the configuration file, restart the service.

For detailed instructions on configuring your server see the following helpful links:

http://askubuntu.com/questions/140126/how-do-i-configure-a-dhcp-server

https://wiki.debian.org/DHCP_Server

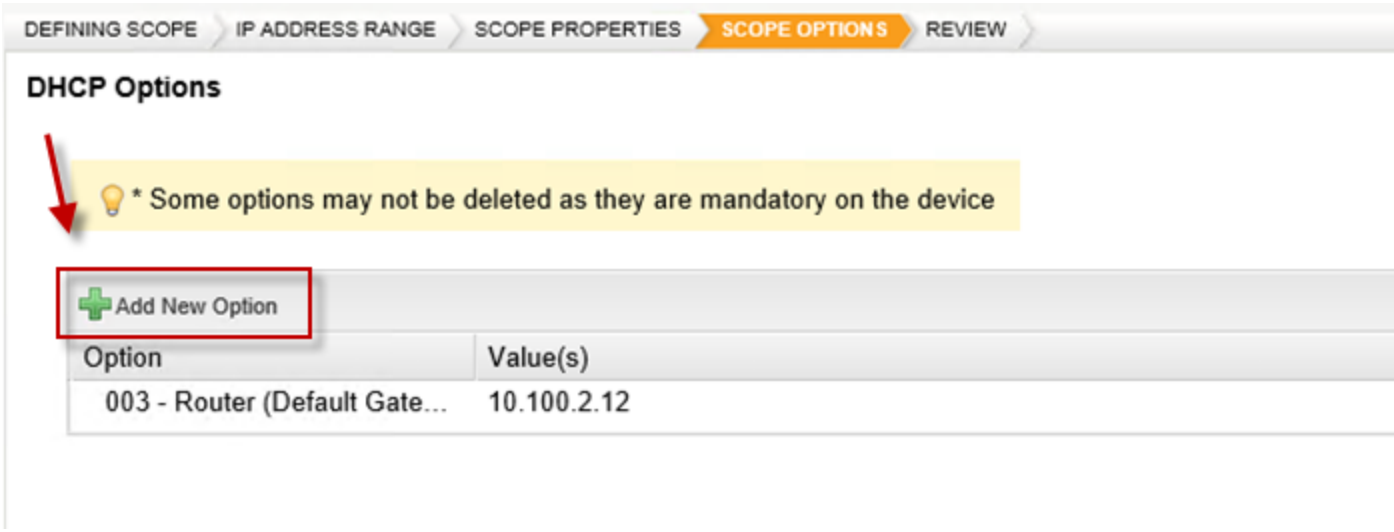
Adding ISC DHCP Servers

To begin managing your ISC servers they must first be added to IPAM. For more information see Adding DHCP Servers to IPAM

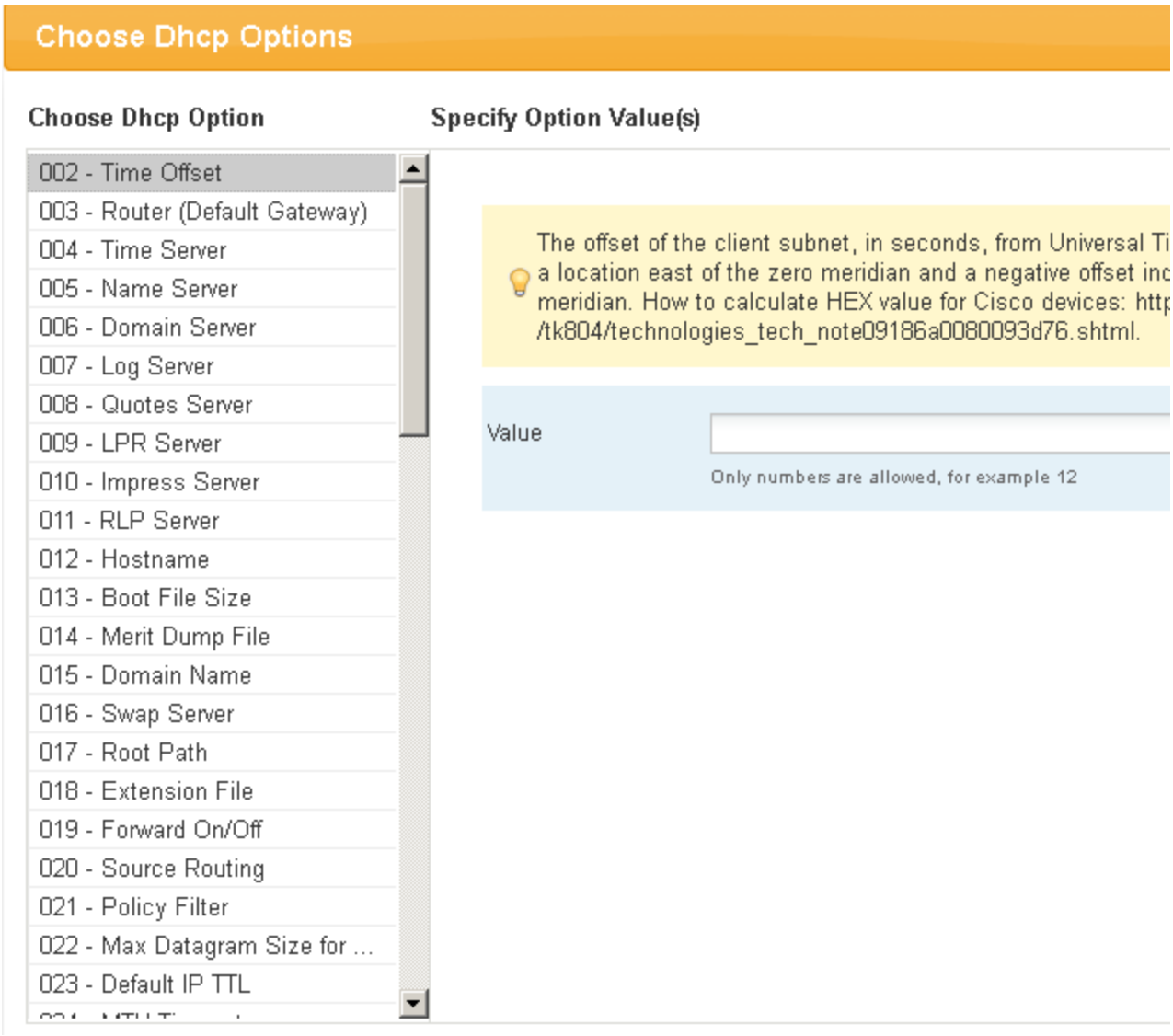
IPAM DHCP Options

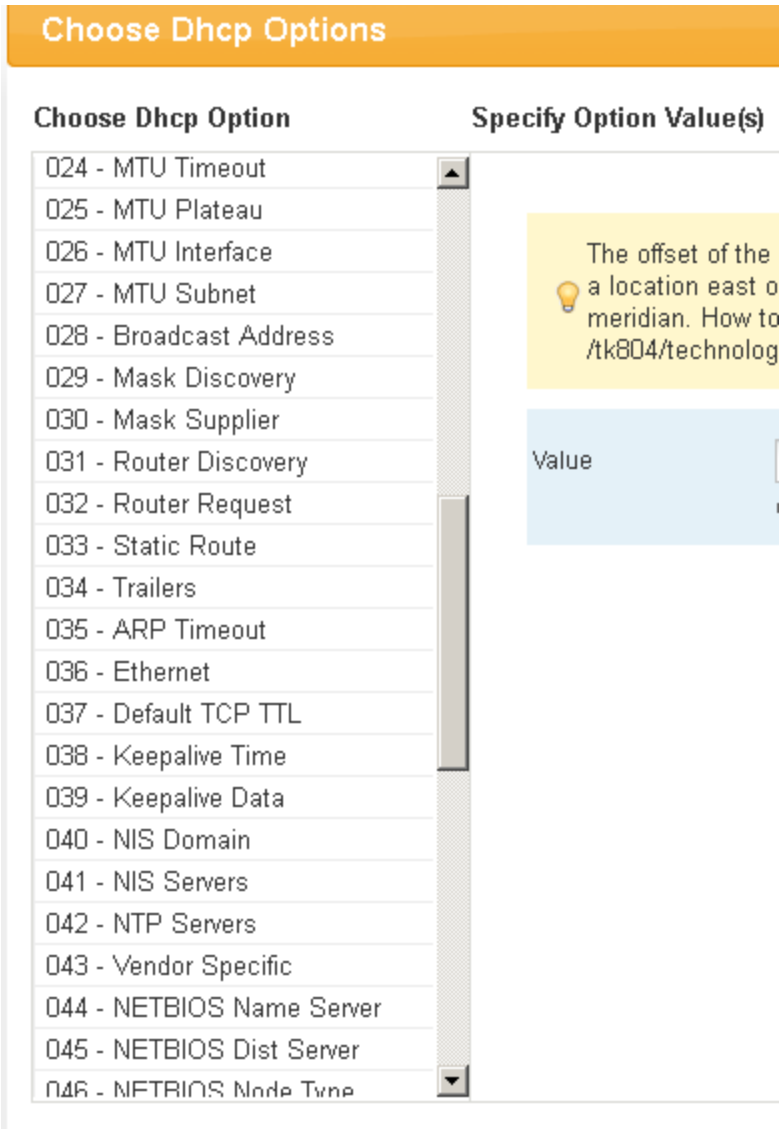
IPAM supports the majority of DHCP scope options defined within the RFC 2132 standard. You will see these options when you are adding a scope in the options wizard. It's the 4th step in the process when adding a DHCP Scope.

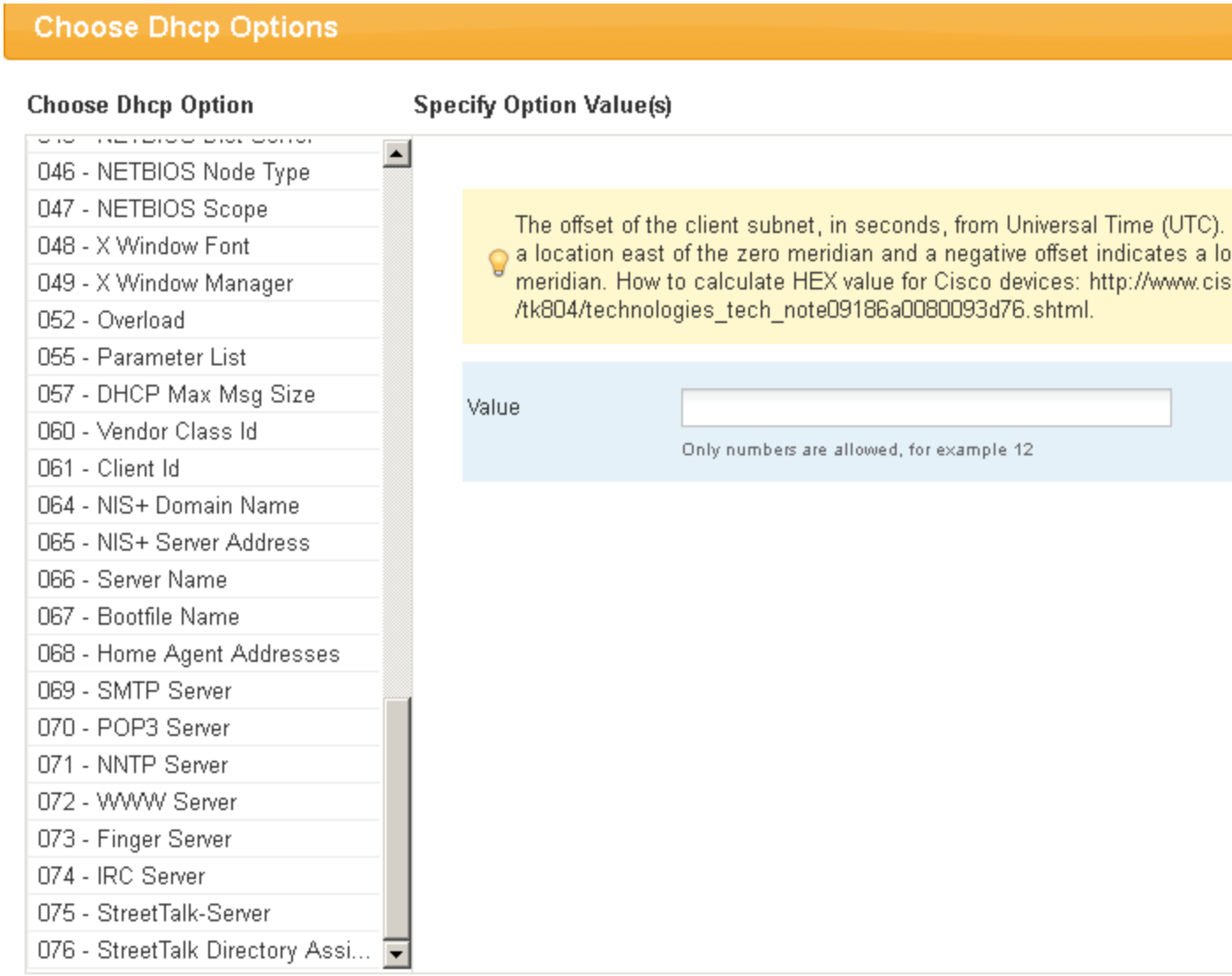
The available options vary based on vendor. The options can be selected by clicking **Add**.



A list of available options will display as follows:


Choose Dhcp Options
Choose Dhcp Option
Specify Option Value(s)
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
018 - Extension File
019 - Forward On/Off
020 - Source Routing
021 - Policy Filter
022 - Max Datagram Size for ...
023 - Default IP TTL
The offset of the client subnet, in seconds, from Universal Ti
a location east of the zero meridian and a negative offset inc
meridian. How to calculate HEX value for Cisco devices: http
/tk804/technologies_tech_note09186a0080093d76.shtml.
Value
Only numbers are allowed, for example 12


Choose Dhcp Options
Choose Dhcp Option
Specify Option Value(s)
024 - MTU Timeout
025 - MTU Plateau
026 - MTU Interface
027 - MTU Subnet
028 - Broadcast Address
029 - Mask Discovery
030 - Mask Supplier
031 - Router Discovery
032 - Router Request
033 - Static Route
034 - Trailers
035 - ARP Timeout
036 - Ethernet
037 - Default TCP TTL
038 - Keepalive Time
039 - Keepalive Data
040 - NIS Domain
041 - NIS Servers
042 - NTP Servers
043 - Vendor Specific
044 - NETBIOS Name Server
045 - NETBIOS Dist Server
The offset of the
a location east o
meridian. How to
/tk804/technolog
Value



Note: Setup Voip Options (66 & 67) on your scopes.

Unsupported DHCP Options:

Microsoft Windows Options

The following options are unsupported:

39 TCP Keepalive Data

58 Renewal Time Value

59 Rebinding Time Value

- There is no UI option to create option 58 & 59 on a Windows DHCP server.
- Options 58 and 59 cannot be set directly, they are simply a function of lease time(option 51).
- Option code 39 only works with Windows2003 devices.

Cisco 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

67 BootFile Name

For more information: http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/dhcp.html#wp1170748

For more information: http://www.cisco.com/en/US/docs/security/asdm/6_2f/user/guide/dhcp_dns.html#wp1284381

ISC Options:

50 Address Request

53 DHCP Message Type

54 DHCP Server Identifier

56 DHCP Message

58 Renewal Time

59 Rebinding Time

Creating DHCP Scopes

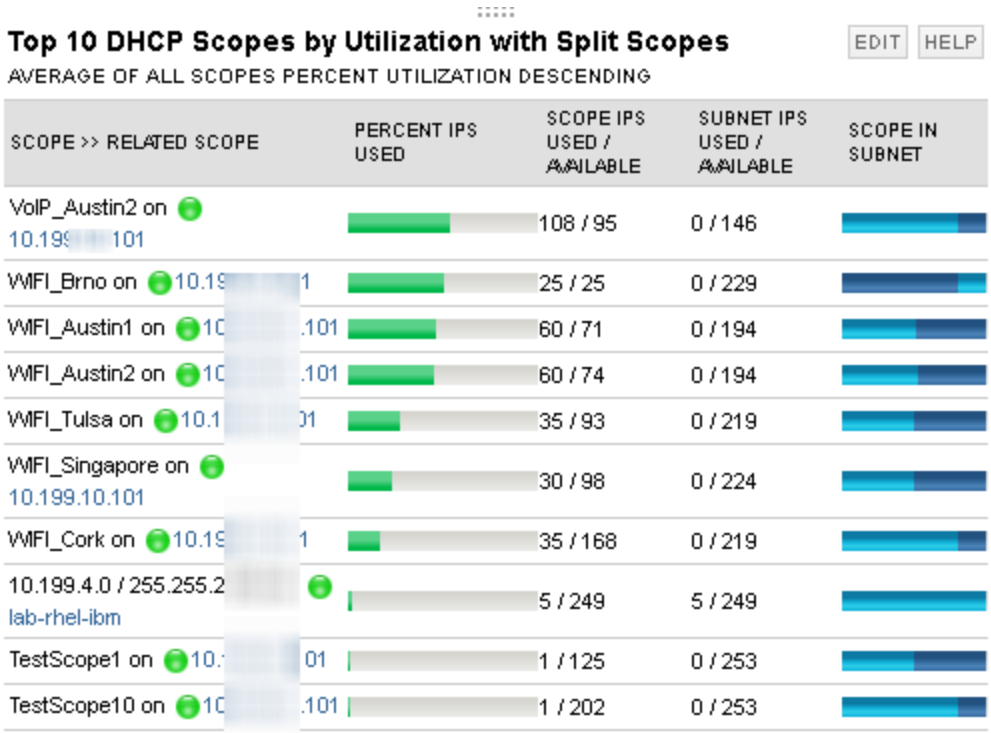
A scope is a consecutive range of IP addresses that a DHCP server is allowed to lease to a DHCP client. Defining one or more scopes on your DHCP servers allows the server to manage the distribution and assignment of IP address to DHCP clients.

The process for adding and editng scopes is simple.

Select from the list of DHCP Servers to Add a Scope and follow the tabs as needed.

The interface options with vary depending on the Vendor you select.

The IPAM Summary page displays the **Top 10 DHCP Scopes by Utilization with Split Scopes Resource**.

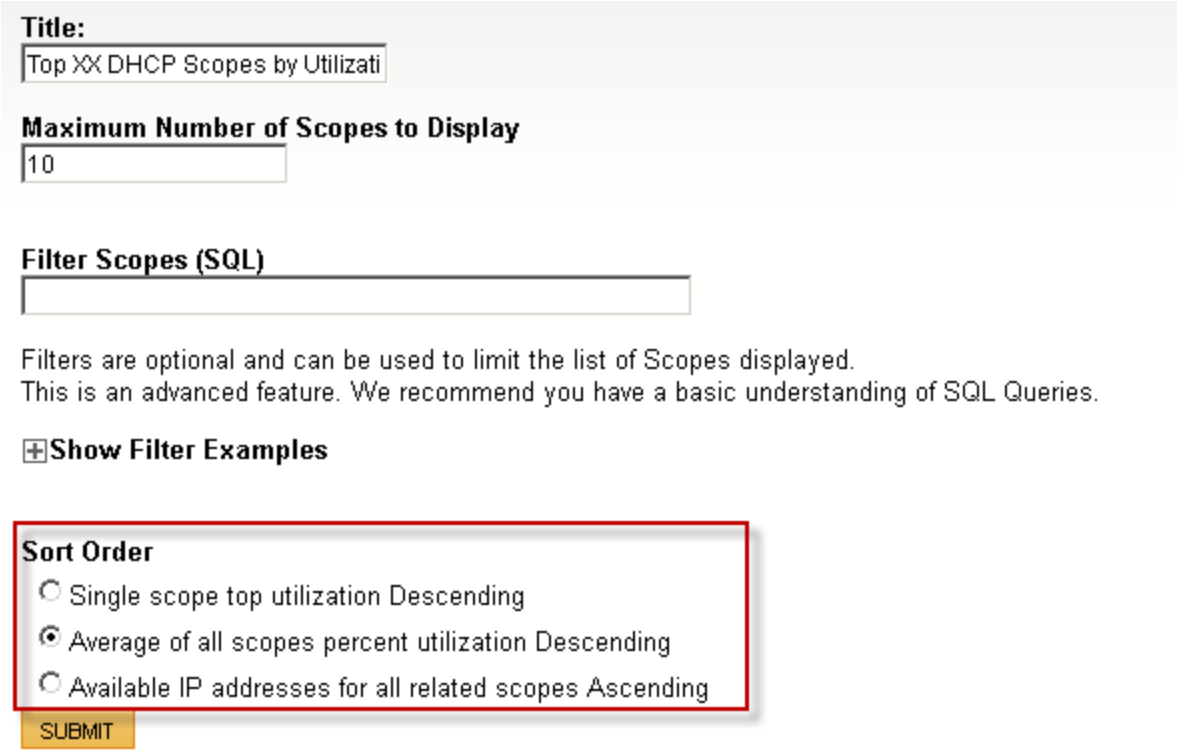


Top 10 DHCP Scopes by Utilization with Split Scopes EDIT HELP

AVERAGE OF ALL SCOPES PERCENT UTILIZATION DESCENDING

SCOPE >> RELATED SCOPE	PERCENT IPS USED	SCOPE IPS USED / AVAILABLE	SUBNET IPS USED / AVAILABLE	SCOPE IN SUBNET
VoIP_Austin2 on 10.199 101		108 / 95	0 / 146	
WIFI_Brno on 10.19 1		25 / 25	0 / 229	
WIFI_Austin1 on 10 .101		60 / 71	0 / 194	
WIFI_Austin2 on 10 .101		60 / 74	0 / 194	
WIFI_Tulsa on 10.1 01		35 / 93	0 / 219	
WIFI_Singapore on 10.199.10.101		30 / 98	0 / 224	
WIFI_Cork on 10.19 1		35 / 168	0 / 219	
10.199.4.0 / 255.255.2 lab-rhel-ibm		5 / 249	5 / 249	
TestScope1 on 10. 01		1 / 125	0 / 253	
TestScope10 on 10 .101		1 / 202	0 / 253	

You can edit the resource by selecting a sort order and by using SQL Filters to limit the which scopes are displayed.



For more information about DHCP Scopes:

- DHCP Split Scopes
- Add new DHCP Scope
- Add new Found DHCP Scope
-

Top Utilization of DHCP Scopes

Scenario: If you are using DHCP Split scopes for high availability or load balancing purposes.

IPAM provides this view that displays the amount of free IP addresses remaining in the subnet of the scope.

This resource displays the top utilized scopes.and if they are split scopes, their split ratio or siblings delineation.

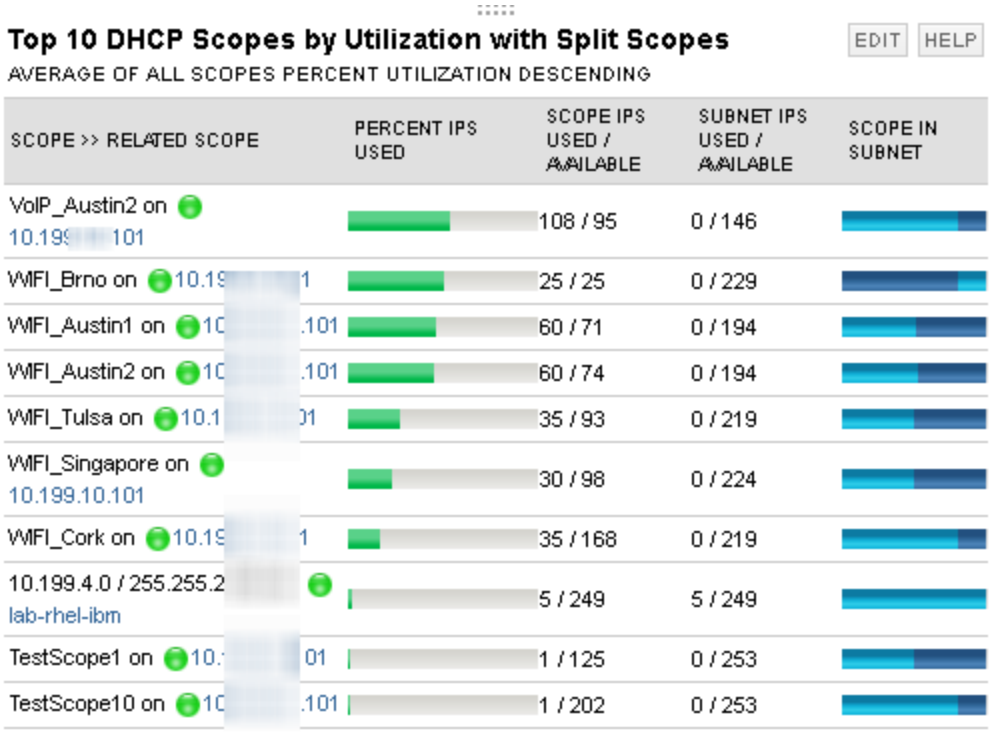
For more information see See "DHCP Split Scopes" on page 94

DHCP Split Scopes

Split scopes can be used to for several reasons:

- Provide load balancing between two DHCP servers
- Ensure high availability DHCP services for your network.

The IPAM Summary page displays the **Top 10 DHCP Scopes by Utilization with Split Scopes Resource**.

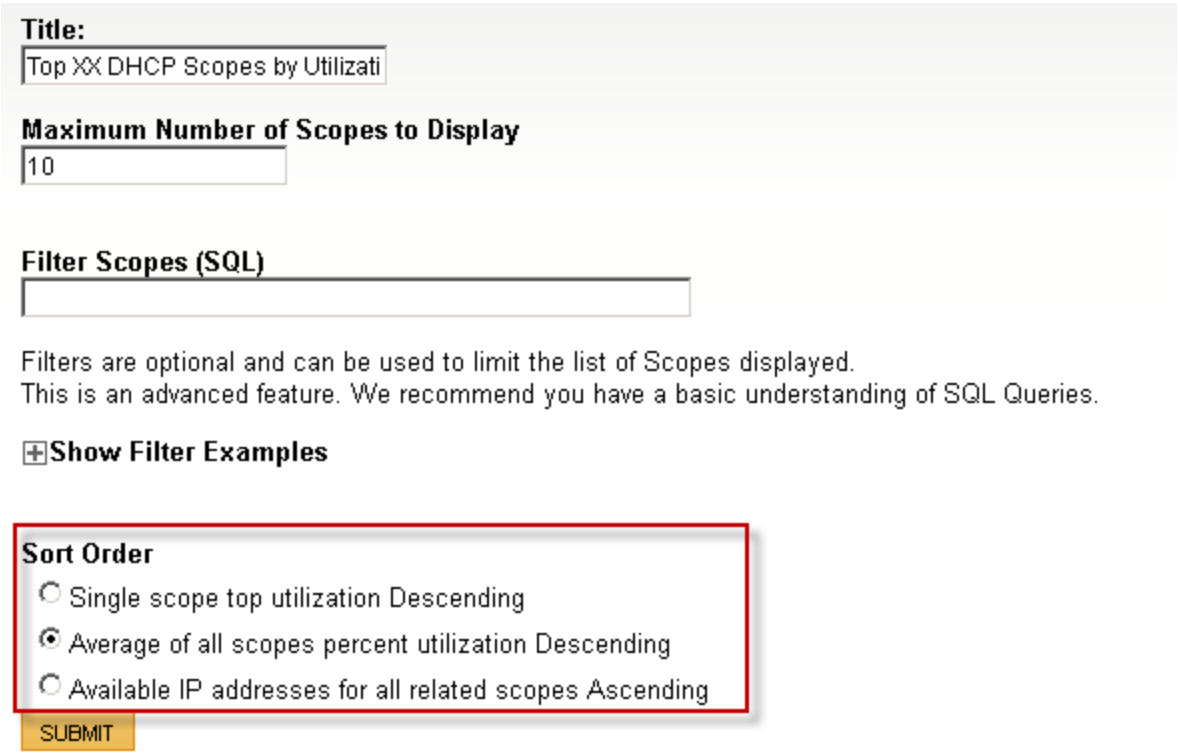


Top 10 DHCP Scopes by Utilization with Split Scopes EDIT HELP

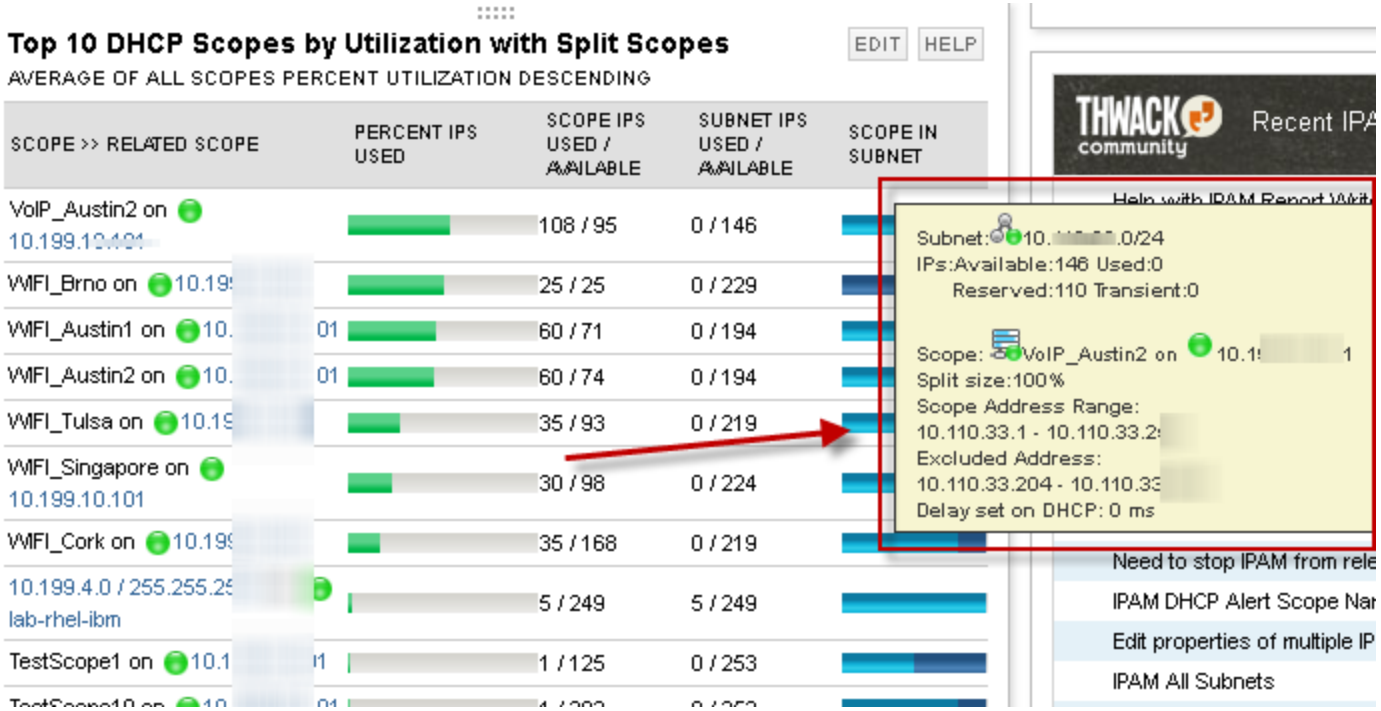
AVERAGE OF ALL SCOPES PERCENT UTILIZATION DESCENDING

SCOPE >> RELATED SCOPE	PERCENT IPS USED	SCOPE IPS USED / AVAILABLE	SUBNET IPS USED / AVAILABLE	SCOPE IN SUBNET
VoIP_Austin2 on 10.199 101		108 / 95	0 / 146	
WIFI_Brno on 10.19 1		25 / 25	0 / 229	
WIFI_Austin1 on 10 .101		60 / 71	0 / 194	
WIFI_Austin2 on 10 .101		60 / 74	0 / 194	
WIFI_Tulsa on 10.1 01		35 / 93	0 / 219	
WIFI_Singapore on 10.199.10.101		30 / 98	0 / 224	
WIFI_Cork on 10.19 1		35 / 168	0 / 219	
10.199.4.0 / 255.255.2 lab-rhel-ibm		5 / 249	5 / 249	
TestScope1 on 10. 01		1 / 125	0 / 253	
TestScope10 on 10 .101		1 / 202	0 / 253	

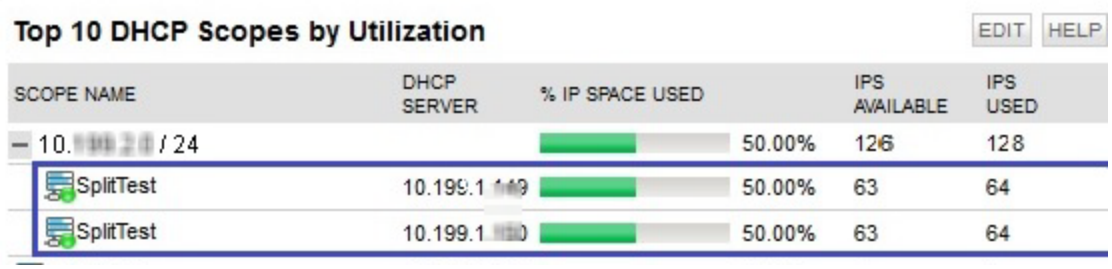
You can edit the resource by selecting a sort order and by using SQL Filters to limit the which scopes are displayed.



Mousing over a scope displays a Tool Tip window.



When you split a scope, the primary server is responsible for a certain group of IP addresses, and the secondary is responsible for the remainder. An offer delay (generally between 1000 and 5000 milliseconds) is set for the secondary server to ensure that if the primary server is unable to provide an IP address within the offer delay time, the secondary server will do so using its pool of addresses.



Scopes are usually split into one of two configurations:

- 50/50, where 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, where 80% of the IP addresses are on the primary DHCP server and only 20% are on the secondary server. This configuration is generally to ensure high availability.

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

You start with a scope01 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.

Now, scope01 will still span the entire subnet, but will exclude the last 20% of the addresses in that subnet (10.10.10.204-254). Scope02 will also span the entire subnet, but will exclude the first 80% of the addresses in that subnet (10.10.10.1-203).

Note:

- Splitting scopes on some Cisco DHCP servers may require you to perform additional configuration steps on the servers themselves.
- You must have two DHCP servers of the same type to split a scope between them.

Adding DHCP Nodes

The following procedure details the steps required to add a Node for monitoring in the IPAM Web Console.

To add a device for monitoring in the IPAM Web Console:

1.Log in to the IPAM Web Console as an administrator.

2.Click **Settings** in the top right of the web console.

3.Click **Manage Nodes** in the Node & Group Management grouping of the Orion Website Administration page.

4.Click **Add Node** on the Node Management toolbar.

5.Provide the hostname or IP Address of the node you want to add in the **Hostname or IP Address** field.

6.***If the IP address of the node you are adding is dynamically assigned,*** check **Dynamic IP Address**.

7.***If you only want to use ICMP to monitor node status, response time, or packet loss for the added node,*** check **ICMP (Ping only)**.

8.***If you want to add an External node to monitor a hosted application with Orion Application Performance Monitor,*** check **External**.

Note: The External status is reserved for nodes hosting applications that are to be monitored with Orion Application Performance Monitor. Orion IPAM will not collect or monitor any data about a node itself, if it is marked as External,.

9.***If you are adding a Cisco UCS Manager,*** check **UCS manager credentials**, and then complete the following steps to provide required UCS credentials in the UCS credentials area.

a.Provide the **Port** on which the UCS manager listens for SNMP queries.

b.Provide an appropriate **User name** and a **Password to gain access to your UCS device**.

c.Click **Test** to confirm the UCS credentials you have provided.

10.***If you are adding a VMware device,*** check **Poll for VMware** to ensure that Orion NPM acquires any data the VMware device provides to SNMP polling requests, and then complete the following steps to provide required vCenter or ESX Server credentials.

a.Select an appropriate **vCenter or ESX credential**.

Notes:

- ***If you are creating a new credential,*** select **<New Credential>**.
- ***If you are editing an existing credential,*** select the credential you want to edit.

SolarWinds recommends against using non-alphanumeric characters in VMware credential names.

b.***If you are creating a new credential,*** provide a **Credential name.**

c.Provide an appropriate **User name** and a **Password**, and then provide the password again in the **Confirm password** field.

d.Click **Test** to confirm the VMware credentials you have provided.

11.***If you want to use SNMP to monitor the added node,*** confirm that **ICMP (Ping only)** is cleared, and then complete the following steps:

a.Select the **SNMP Version** for the added node.

Notes:

- Orion uses **SNMPv2c** by default. If the device you are adding supports or requires the enhanced security features of SNMPv3, select **SNMPv3**.

If SNMPv2c is enabled on a device you want Orion IPAM to monitor, by default, Orion IPAM will attempt to use SNMPv2c to poll for performance information. If you only want Orion IPAM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

b.***If you have installed multiple polling engines,*** select the **Polling Engine** you want to use to collect statistics from the added node.

Note: This option may not be available if you are only using one polling engine to collect information from your network.

c.***If the SNMP port on the added node is not the Orion default of 161,*** provide the actual port number in the **SNMP Port** field.

d.***If the added node supports 64bit counters and you want to use them,*** check **Allow 64bit counters**.

Note: Orion fully supports the use of 64-bit counters; however, these high capacity counters can exhibit erratic behavior depending on manufacturer implementation. If you notice peculiar results when using these counters, use the Node Details view to disable the use of 64-bit counters for the device and contact the hardware manufacturer.

12.***If you want Orion to use SNMPv2c to monitor the added node,*** provide valid community strings for the added node.

Note: The **Read/Write Community String** is optional, but Orion does require the **public Community String**, at minimum, for node monitoring. If you want to use read/write SNMPv3 credentials, complete the following steps in the Read / Write SNMPv3 Credentials area.

13.*If you want Orion to use SNMPv3 to monitor the added node,* provide the following **SNMP Credentials**, **Authentication**, and **Privacy/Encryption** settings:

- **SNMPv3 Username**, **Context**, **Authentication Method**, and **Password.**

Note: If this password is a key, check Password is a key.

- **SNMPv3 Privacy/Encryption Method** and **Password**.

Note: If this password is a key, check Password is a key.

14.*If you want to save the provided credentials as a credential set,* provide a **Name**, and then click **Save**.

15.*If you want to delete a currently saved credential set,* select the set to delete, and then click **Save**.

16.*If you are using SNMP to communicate with your added node,* click **Validate SNMP** after entering all credentials to confirm your SNMP settings.

17. Click **Next**.

18.Check the objects for the added node that you want Orion to monitor or manage. The following options are available in the selection toolbar:

- Clicking **All** selects all listed devices and charts for monitoring.
- Clicking **None clears any checked** interfaces, volumes, or interface charts **that have been selected for monitoring.**
- Clicking **All Volumes selects all listed volumes for monitoring.**

19.After you have selected objects for monitoring, click **Next**.

20.***If Orion NPM is installed and you want to apply pollers to the added node,*** click **+** to expand poller groups, as necessary, check the appropriate pollers, and then click **Next**.

Note: For more information about using predefined pollers or about defining your own universal device pollers, see "Monitoring MIBs with Universal Device Pollers" in the SolarWinds Orion Network Performance Monitor Administrator Guide.

21.***If you want to edit the SNMP settings you provided earlier,*** change the appropriate values in the SNMP area of the Change Properties page, and then click **Validate SNMP** to confirm your new settings.

22.***If you want to edit the default polling settings for your added node,*** change the **Node Status Polling** or **Collect Statistics Every** values in the Polling area of the Change Properties page, as appropriate.

Note: The **Node Status Polling** value refers to the number of seconds, between the node status checks Orion performs on the added node. The **Collect Statistics Every** value refers to the period of time between the updates Orion makes to displayed statistics for the added node.

23.***If you have defined any custom properties for monitored nodes,*** provide appropriate values for the added node in the Custom Properties area of the Change Properties page.

Note: The Custom Properties area is empty if you have not defined any custom properties for monitored network objects.

24.Click **OK, Add Node** when you have completed properties configuration.

25.***If you have successfully added the node,*** click **OK** on the dialog.

Adding DHCP Servers to IPAM

After you have added your DHCP server as a Node you can now add the server to IPAM.

Windows DHCP Server Requirments.

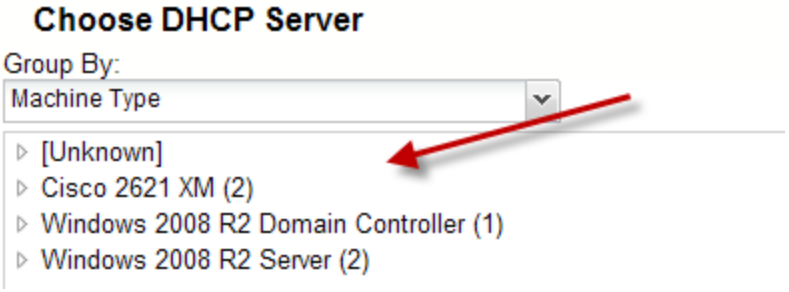
For Cisco requirements click here.
For ISC requirements click here.
For BIND requirments click here.

To add and configure s DHCP server:

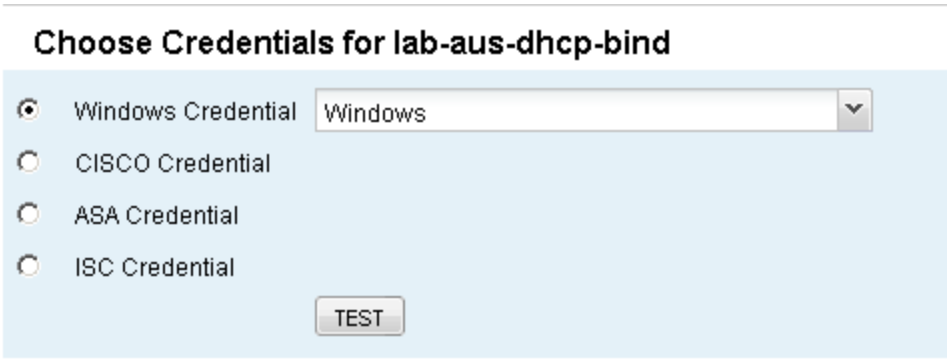
1.Click on the **DHCP & DNS Monitoring** tab.

2.Click **Add New DHCP Server**.

3.Select the DHCP node to be added from the list of nodes.



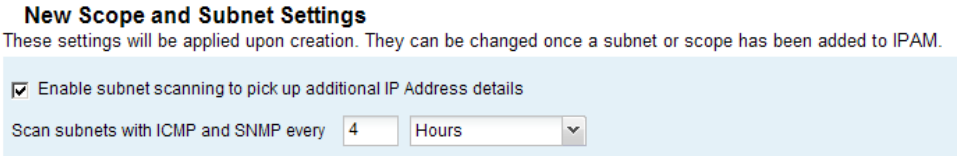
4.Choose or create the necessary credentials from the drop down list. Then click **Test** to verify the credential.



5.Select the **DHCP Server Scan Settings**. Default is set to 4 hours.

6.***If you want to automatically add new scopes and subnets after scanning***, check the box.

7. ***If you want IPAM to scan for additional IP Address details using ICMP and SNMP,*** check the **Enable subnet scanning to pick up additional IP Address details** box and select the scanning interval.



8.To finish, click **Add DHCP Server**

Note:

- All Windows credentials are sent in clear text during configuration only. Consider updating credentials while locally logged into the IPAM server or over an HTTPS connection.

The Windows account specified within IPAM 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 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.

Editing DHCP Servers

The following procedure edits the properties of an existing DHCP Server.

To edit an existing DHCP Server:

1.Click the DHCP & DNS Monitoring tab.

2.Select the DHCP Server that you want to edit by checking the box.

3.Click **Edit Server**.

4.Edit as necessary and then click **Save**.

Note: The edited properties are fields specific to IPAM and not related to any data in the DHCP server.

Removing DHCP Servers

The following procedure will remove an existing DHCP Server from the IPAM web console.

To remove an existing DHCP Server:

1.Click the DHCP Servers tab.

2.Select the DHCP Servers that you want to remove by checking the boxes.

3.Click **Remove Servers**.

4.Click **Delete Listed Items.**

Deleting Devices from Monitoring

The following procedure deletes devices (nodes) from monitoring in the web console.

Warning: Deleting nodes from monitoring in the web console automatically terminates monitoring of all applications, interfaces, and volumes on the deleted nodes.

Note: You can select multiple devices to delete at the same time. Additionally, using the search tool above the node list, you can select multiple interfaces on different nodes for simultaneous deletion.

To delete devices from monitoring in the IPAM Web Console:

1.Log in to the IPAM Web Console as an administrator.

2.Click **Settings** in the top right of the web console, and then click **Manage Nodes** in the Node & Group Management grouping of the Orion Website Administration page.

3.***If you want to delete a node and all its applications, interfaces, and volumes from monitoring,*** complete the following steps.

a.Locate the node to delete using either of the following methods:

- Use the search tool above the node list to search your Orion database for the node you want to delete.

Select an appropriate **Group by:** criterion, and then click the appropriate group including the node to delete.

b.Check the node to delete in the list, and then click **Delete** on the toolbar.

4.***If you want to delete a monitored application, interface, or volume,*** use the following steps.

a.Locate the element to delete using either of the following methods:

- Use the search tool above the node list to search your Orion database either for the parent node of the object to delete or for the object itself.

Select a **Group by:** criteria, and then click the appropriate group including the parent node of the object to delete.

b.***If you have a list of node results,*** click **+** to expand the parent node of the object you want to delete.

c.Check the object to delete, and then click **Delete** on the toolbar.

5.Click **OK** to confirm deletion.

DHCP Graph View

The Graph View presents a graphical representation of the selected DHCP Servers IP Address percentage use. Unless certain Scopes/Servers are selected, the DHCP graph view will collect statistics for what is visible in the current tab.

To view a DHCP Server Graph View:

1.Click the DHCP Servers tab.

2.Select the DHCP Servers that you want to graph by checking the boxes.

3.Click **Graph View**.

DHCP Scopes Management

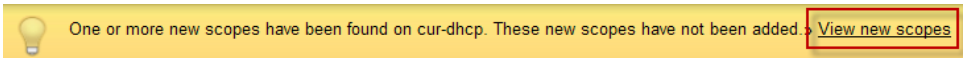
The following sections detail how to create, edit, split, and remove DHCP Scopes in IPAM.

The **DHCP & DNS Management** tab > **DHCP Scopes** tab allows you to choose from several options:

- Add new DHCP Server
- Add new DHCP Scope
- Add new Found DHCP Scope
- DHCP Split Scopes
- DHCP Reservations

Adding DHCP Scopes

The following procedure adds a new DHCP Scope. IPAM will also find scopes during scans. Found scopes will appear in the **Found DHCP Scope** dropdown. When IPAM finds a scope a message banner will display.



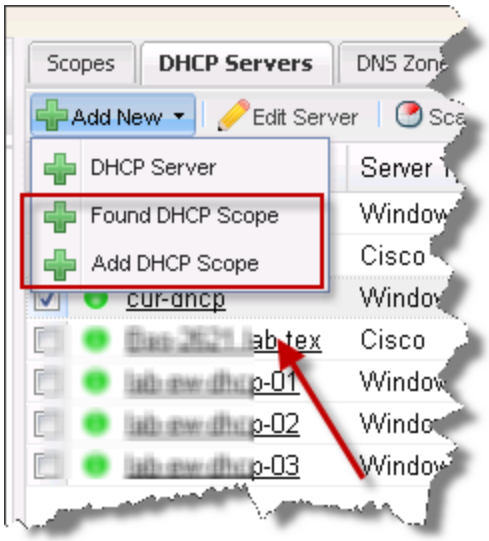
To create a new DHCP Scope:

1.Click DHCP & DNS Scope Monitoring tab.

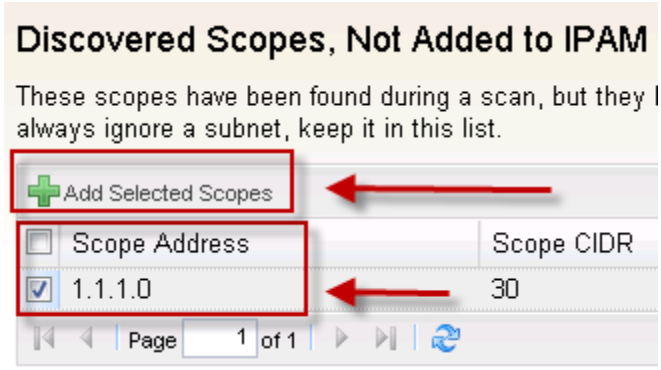
2.Click the **DHCP Servers** tab.

3.Select a (Windows) server.

4.Click Add New > Found DHCP Scope or **Add DHCP Scope.**

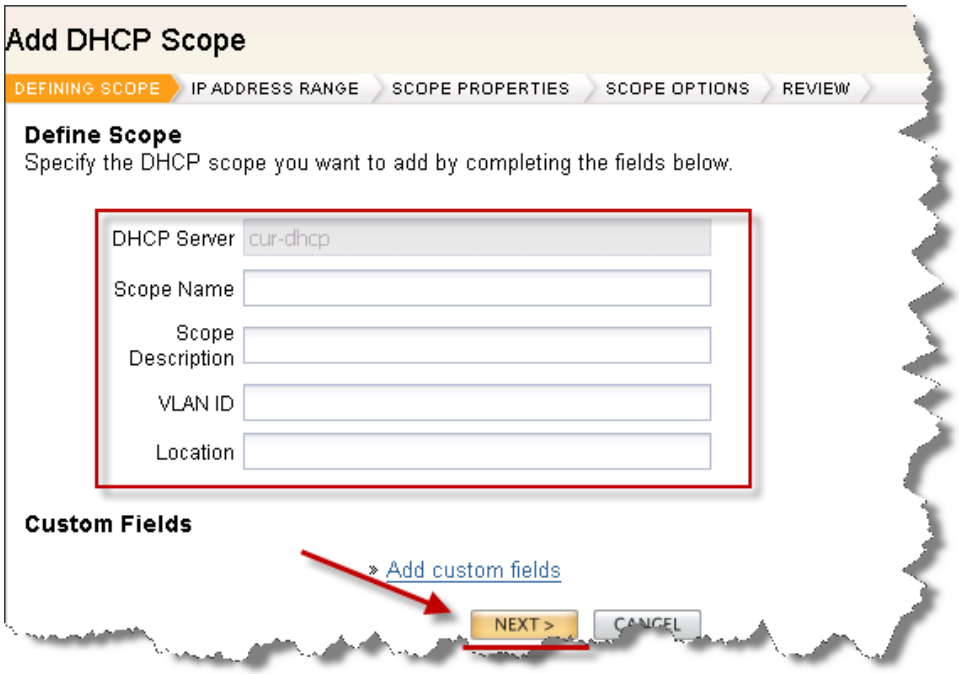


a.***If you are adding a Found Scope – select the Scope and click*** **Add Found Scope**.

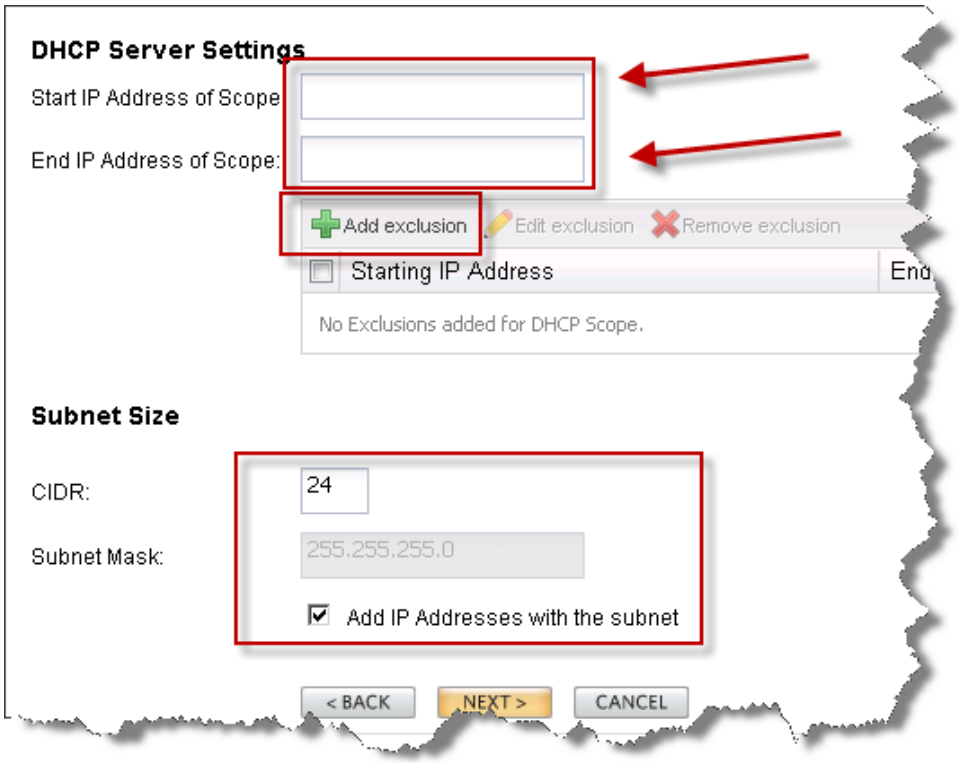


b.***If you are adding a new Scope, click*** **Add New Scope**

c.Define the Scope name, description and any custom fields.

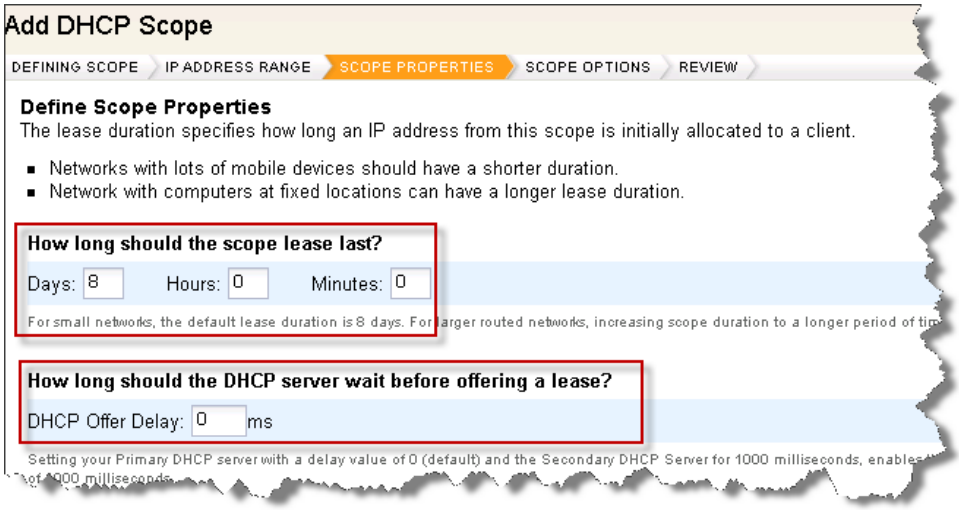


5.Define the Scope ranges, add exclusions and define the CIDR for the new subnet and then click **Next.**



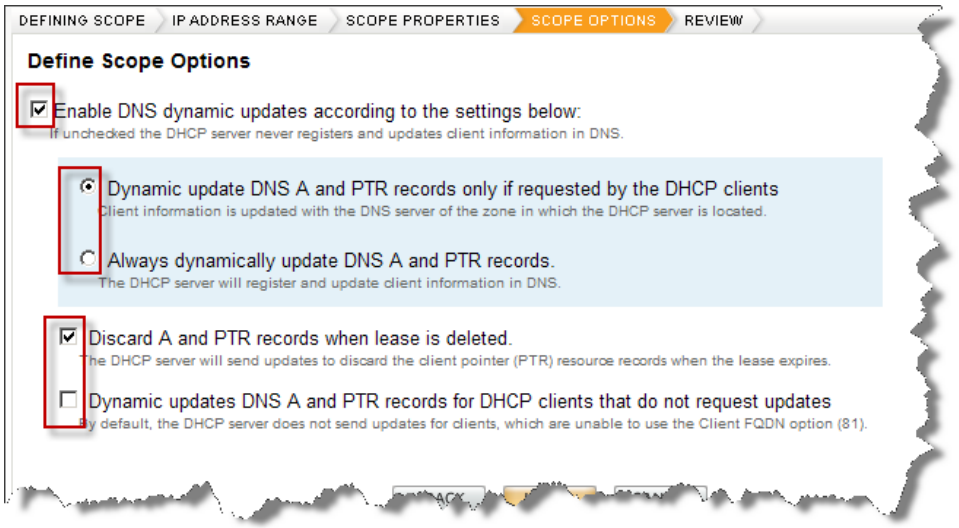
6.Define the Scope Properties by entering the duration of the scope lease.

a.Offer Delay is only supported on Windows 2008 R2. The IPAM server also needs to be on Windows 2008 R2.

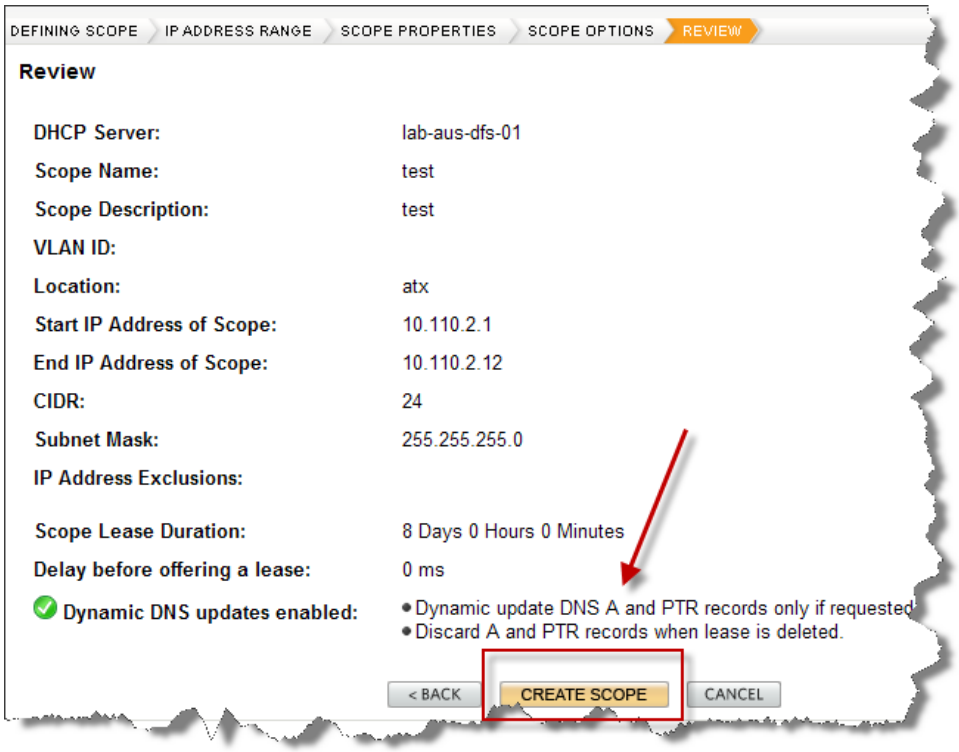


7.Click **Next**.

8.Define the **server** and then click **Next.**



9.Review the Scope details.



10.To finish, click **Create Scope**.

Editing DHCP Scopes

The following procedure edits the scope detail properties of an existing IPAM DHCP Scope.

To edit an existing DHCP Scope:

1.Click **IP Address Manager** in the Menu bar.

2.Click **DHCP & DNS Monitoring**.

3.Click **Scopes**.

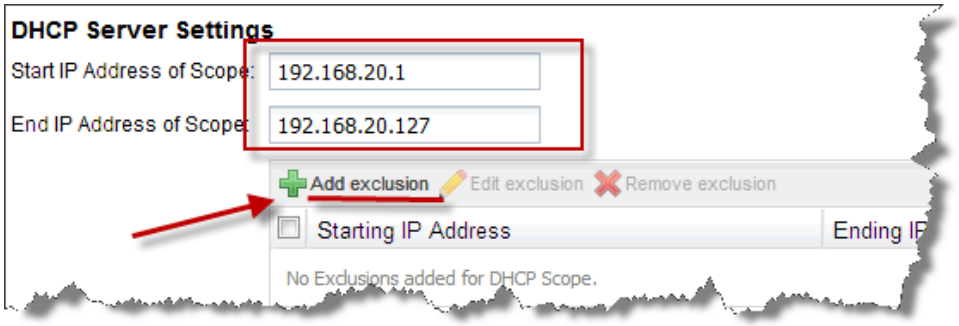
4.Select the Scope Name that you want to edit by using the check box.

5.Click **Edit Scope Details** in the menu bar.

a.You can edit the name/description and or add custom fields.

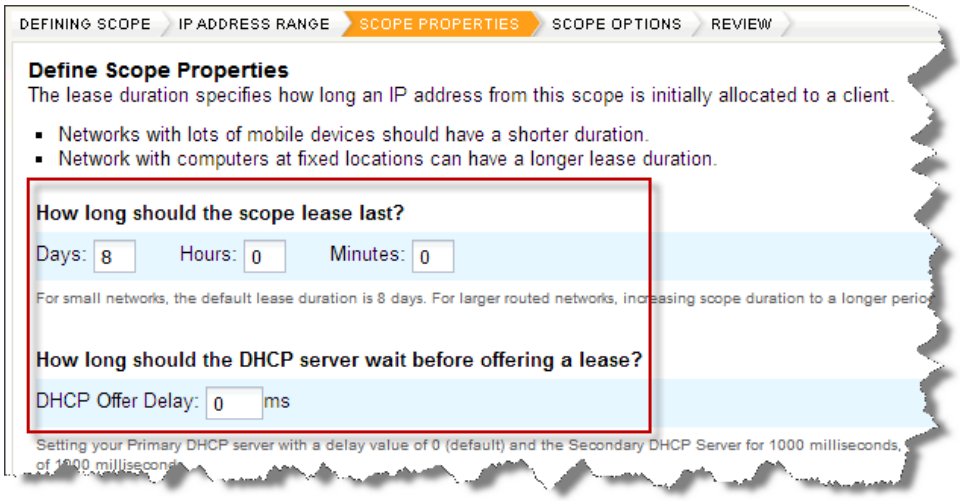
6.Click **Next.**

a.Edit the IP Address range and or click **Add Exclusion**.



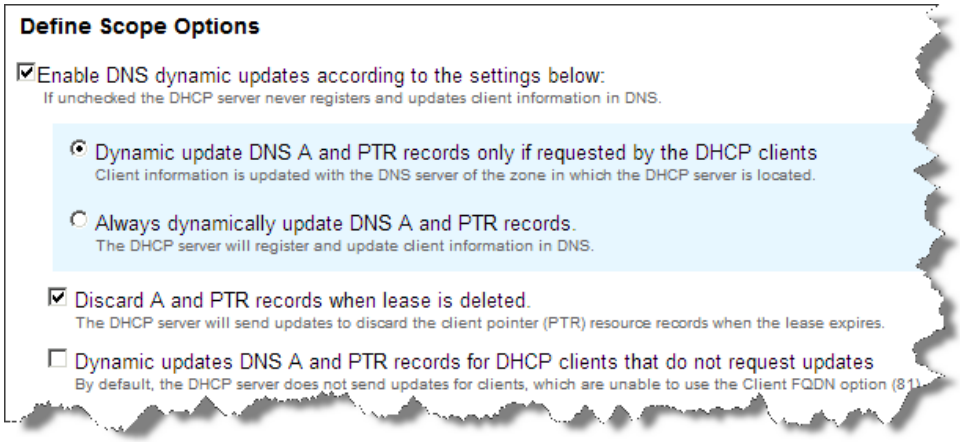
7.Click Next.

8.Define the Lease Duration.



9. Click **Next.**

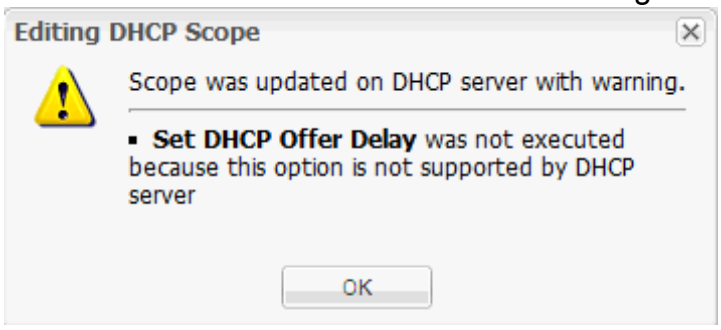
10. Define DNS options as needed.



11.Click **Next.**

12. Review changes and click **Update Scope**.

Note: When editing you may see a popup message if the scope is not a **Windows 2008 R2 DHCP Server**. You can ignore this message.



DHCP Reservations

IPAM allows you to create, update and delete DHCP reservations (static leases).

The following steps detail how to change the reservation status of an IP Address on a Windows DHCP server:

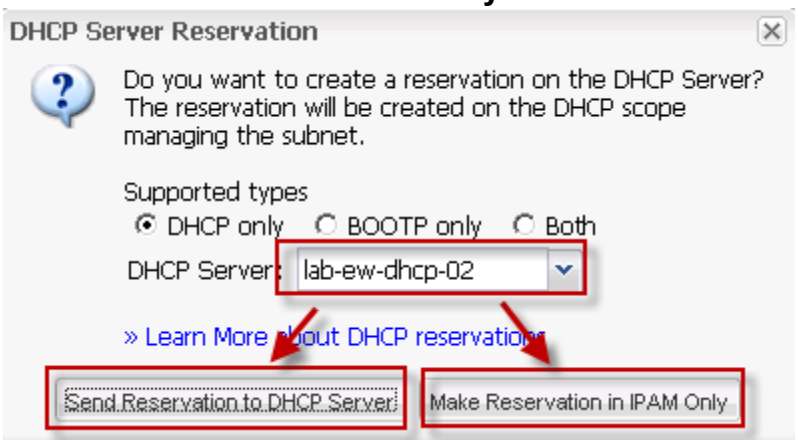
1.**Navigate to the edit IP Address View tab.**

2.Select an IP Address and click **Set Status**, **set Status to Reserved.**

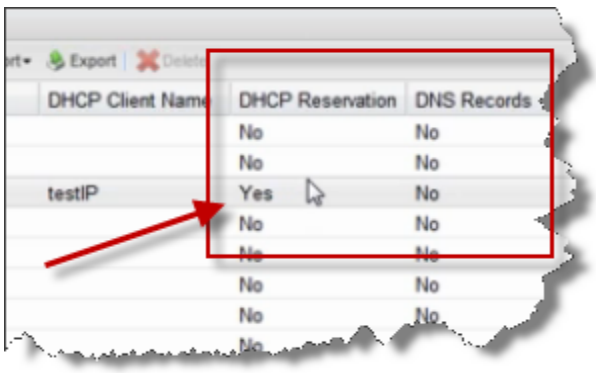
3.**Select the DHCP Server (if needed) and choose where this change is to be in implemented.**

a.Send Reservation to the DHCP Server.

b.Make Reservation in IPAM only.



4.**This column will display the new Reservation status on the DHCP Server.**



Removing Scopes

The following procedure will remove an existing DHCP Scope.

To remove an existing DHCP Scope:

1.Click IP Address Manager in the menu bar.

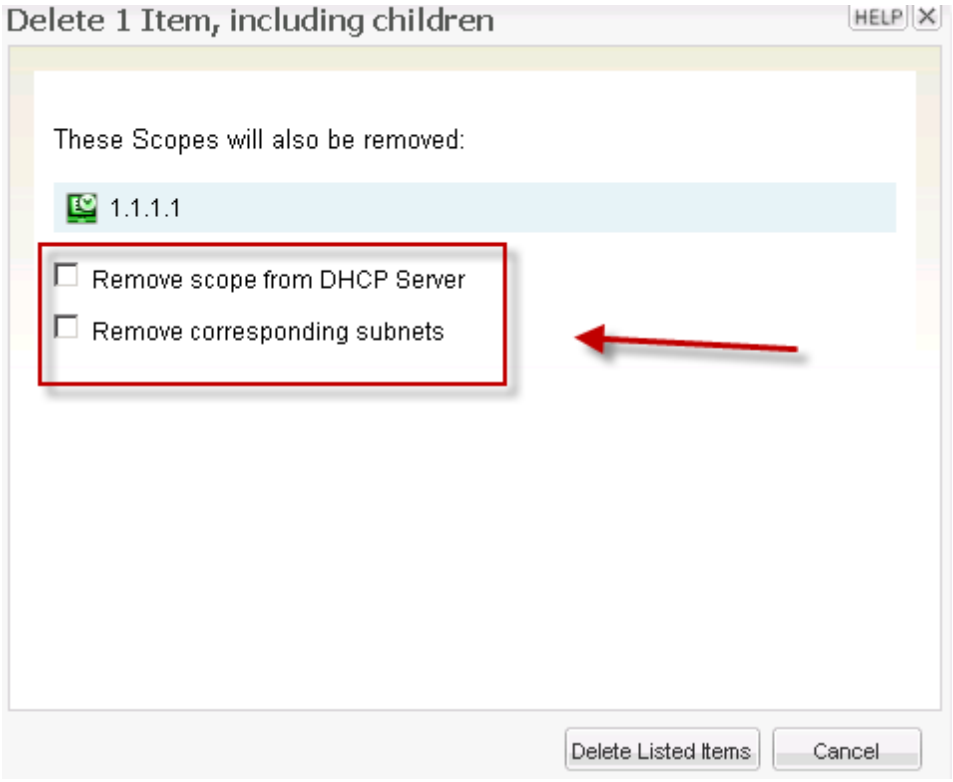
2.Click DHCP Scope & DNS Monitoring.

3.Click Scopes tab.

4.Select the DHCP Scopes that you want to remove by checking the boxes.

5.Click Remove Scopes.

6.Click Delete Listed Items. ***If you want the scope removed from the DHCP Server and or the corresponding subnets removed, check the corresponding boxes.***



Chapter 7: DNS Management

The following chapter details how IPAM can help manage and monitor your DNS servers.

Select from the topics below:
Manually add nodes or add them using Discovery Central
Adding a DNS Server to IPAM
DNS Server WMI Permissions
DNS Zone Transfers
DNS Records
BIND DNS Monitoring and Management
DNS record inconsistencies

Adding a DNS Server

Note: Only Microsoft DNS Servers (Windows 2003, 2008 and 2012) are supported. Some environments may require you to grant read-only access to a non-administrator account. ***For more information see:*** http://knowledgebase.solarwinds.com/kb/questions/3699/

The following steps detail how to add a DNS Server to the IPAM web console. All DNS servers must already exist as nodes in your installation.

To add a DNS Server:

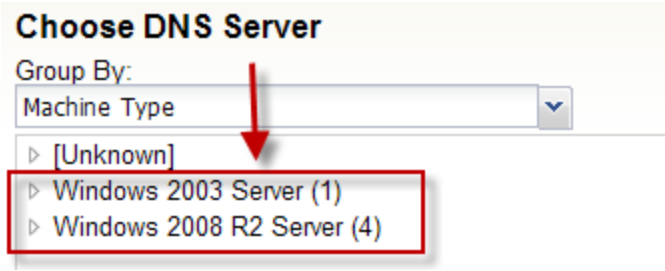
1.Click the **IP Addresses tab**.

2.Click **DHCP & DNS Monitoring**.

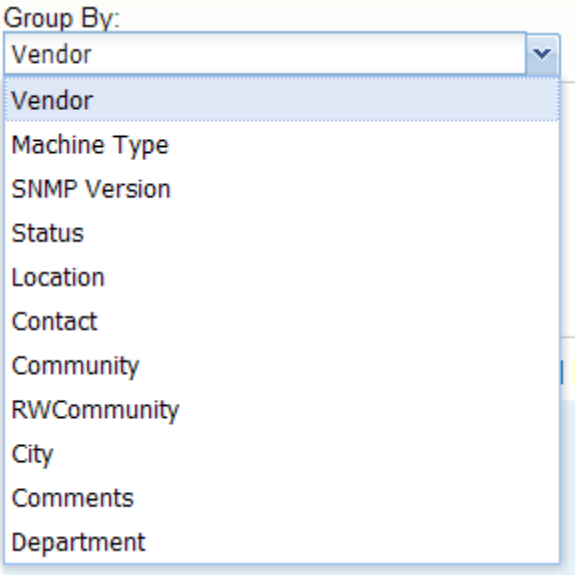
3.Click the **DNS Servers** tab.

4.Click Add new **DNS Server.**

5.Select a DNS Server from the list. If not listed, use the Group By drop down.



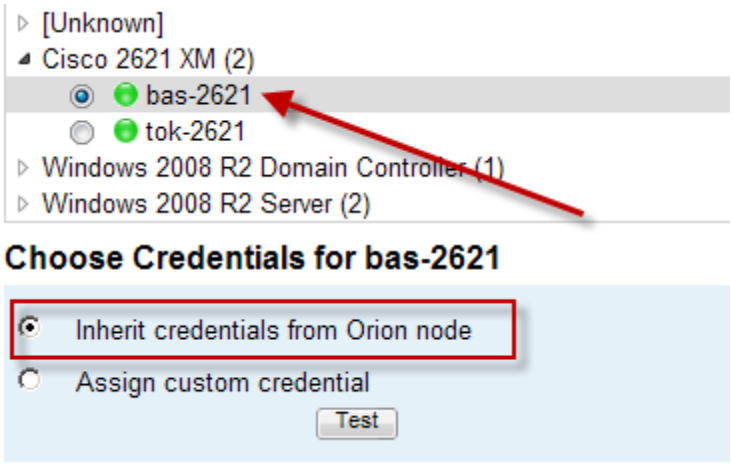
a.Use the **Group By** dropdown to sort the DNS servers listed.



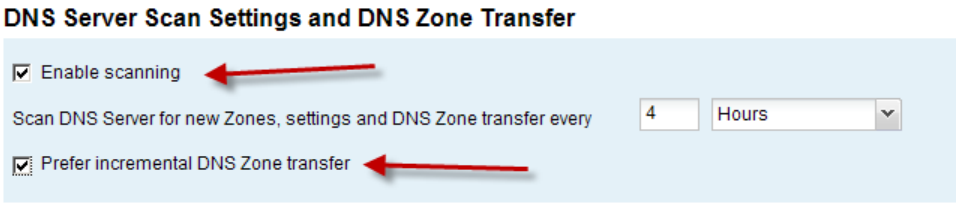
6.Choose the credentials to use.WMI credentials can be inherited from node to DNS server.

a.Provide the user name and password, and then confirm by clicking **Test**. If you are providing windows credentials for accessing and receiving information through WMI, ensure you provide the account name in the following syntax:

domain Or Computer Name\userName for domain level authentication or userName for workgroup level authentication.

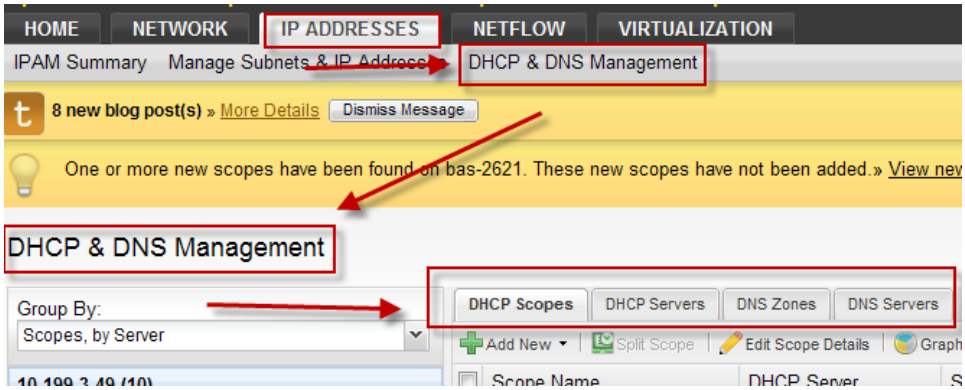


7.**Enable Scanning-** IPAM scans for the DNS Server for new Zones and settings based upon the interval time. Check the box to enable incremental DNS Zone transfers.



8.Click **Add Server.**

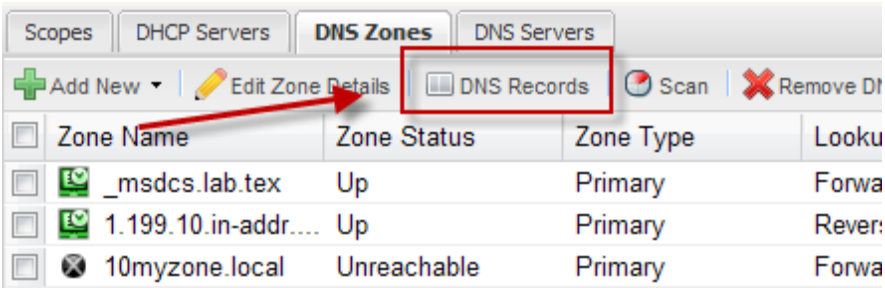
9.Once added it may take some time for DNS Zones to appear. You can navigate using the DNS Zones tab.



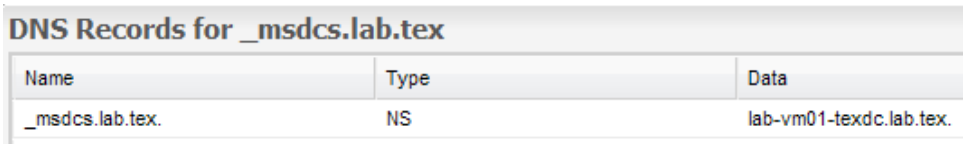
DNS Records

To view DNS records select the DNS Zone Tab.

1.Select a Zone Name and click DNS Records.



2.You will see a popup similar to this:



DNS Server WMI Permissions

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

Enable an Account for WMI:

In order to manage DNS Servers from IPAM you need to have a DNS Server Administrator account that is allowed to make changes on the DNS Server. With a standalone DNS server, this could be a Local Administrator configured for WMI access.

Note: Administrators are by default configured to make DNS Server management tasks. Within the AD & DNS setup, this would be an account with full DACL with remote WMI management enabled.

Granting read only access to non-administrator account for IPAM DNS Monitoring

You may have a scenario where you need to poll the DNS server without an administrator account. One option is add the User to the DNSAdmin group.

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

Configure DCOM Services

1.Start dcomcnfg

2.Expand Component Services\Computers and Right mouse click on My Computer and select Properties.

3.Go to the **COM Security** Tab.

4.In the **Access Permissions** group click on **Edit Default** and add your account and **Enable Local Access** and **Remote Access Checkboxes**.

5.In the **Access** permissions group click on **Edit Limits**, add your account and enable **Local and Remote Access**.

6.In the Launch and Activation permissions click on **Edit Default** and add your account and **Allow all checkboxes**.

7.In the **Launch And Activation permissions** Click on **Edit Limits** and Add your account and **Allow all checkboxes**.

Configure Access to the WMI Branch

1.Start MMC console and add **WMI Control Snapin**.

2.Right click on the snapin and click on **Properties**.

3.In the **Security** Tab select MicrosoftDNS branch and Click on **Security** button.

4.Add your account, and **Allow: Execute Methods, Enable Account, Remote Enable.**

Testing Connection to a DNS Server with specific credentials

Use wbemtest tool and connect to a machine using namespace like:

\\remote_hostname\root\MicrosoftDNS

DNS Zone Transfers

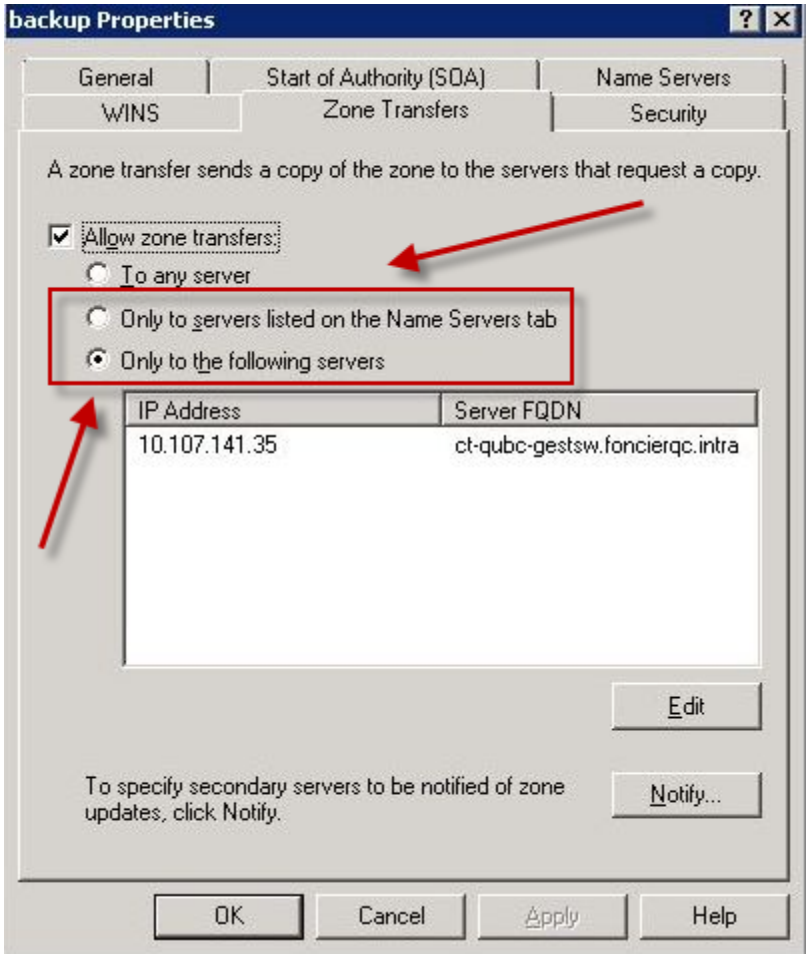
IPAM changes the transfer zone tab by adding the IP Address of the IPAM server. This feature requires an Admin account for adding DNS servers.

When you add a DNS server in IPAM, it changes the **Transfer Zone Configurations** on the DNS server.

For example: If you have the **Allow zone transfers** selected for servers listed on the **Name Servers** Tab, IPAM will set this configuration to **Only to the Following Servers**.

To manually configure your DNS server.

- Verify that **Zone Transfers** are enabled.
- The administrator will need to select the option "**To any server"** or IPAM will default to the option "**Only to the Following Servers"** using the IP Address of the IPAM server.



Editing a DNS Server

To edit a DNS Server:

1.Click the **IP Addresses tab**.

2.Click **DHCP & DNS Monitoring**.

3.Click the **DNS Servers** tab.

4.Click **Edit DNS Server.**

5.Edit the Properties as needed and click **Save.**

Removing DNS Servers

To Remove a DNS Server:

1.Click the **IP Addresses tab**.

2.Click **DHCP & DNS Monitoring**.

3.Click the **DNS Servers** tab.

4.**Select a Server to delete and then** click **Edit DNS Servers.**

5.Click **Delete Listed Items.**

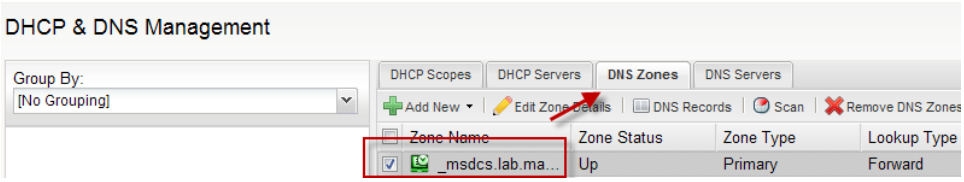
DNS Records

IPAM supports five DNS record types. Each of the five DNS Records can be customized as needed.

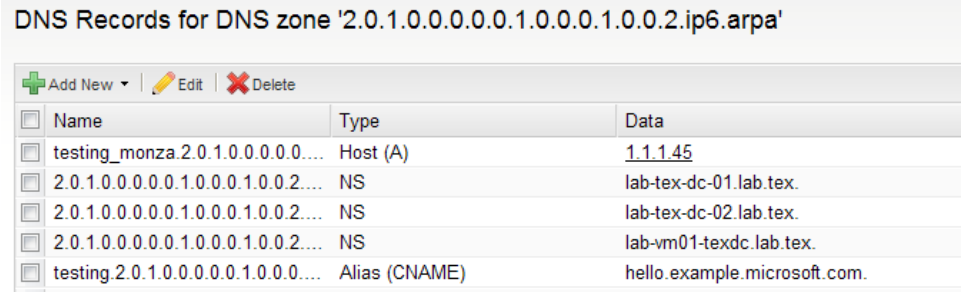
- IPAM automatically detects DNS forward and Reverse mismatches.
- Automatic creation of DNS PTR records when adding new devices into DNS Zones.
- From this location you can manage all aspects of your domains registration. You can also change your domain name servers.

The following steps detail how to edit DNS Records:

1.Select a zone then click a DNS Records

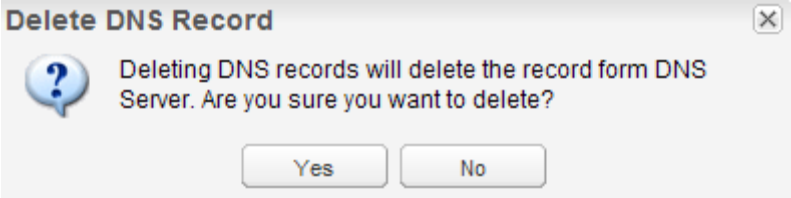


2.A **DNS Records** details page will display.



3.Select a single record to Edit or Add a new record to.

4.***If you want to delete a record, select the record and then click Delete. This message will display before you can proceed.***



DNS Records supported in IPAM.
A Record: An A record gives you the IP address of a domain. Example: www, mail, ftp, webmail, www2, secure, store, dev
AAAA Record: Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.
CNAME Record: CNAME records are used to map aliases with domain names. Example: Record: webmail Address: mail.hostedmail.com
MX Record: MX records should be added when you want to use your external mail servers to process your e-mail. Example: Priority: 10 Record: @ Address: mail.domain.com
PTR Record: A domain name pointer should be used when you want to map a network interface (IP) to a host name.

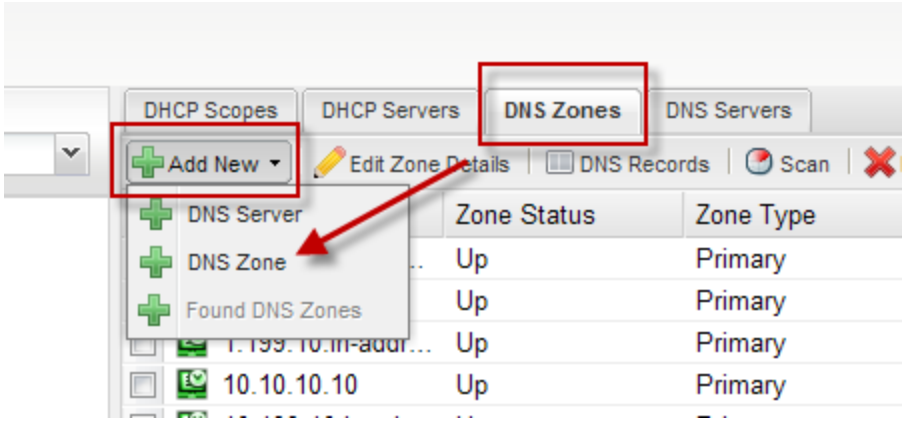
Adding a DNS Zone

The following section details how to add a DNS Zone in IPAM.

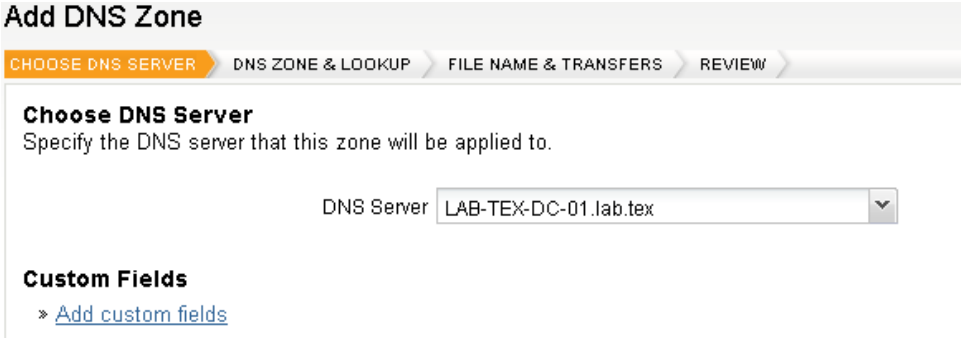
To add a DNS Zone.

1.Click the **DNS Zones** tab.

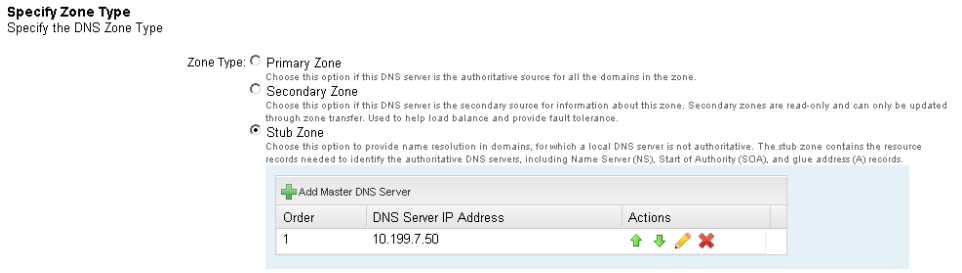
2.Click **Add New > DNS Zone**.



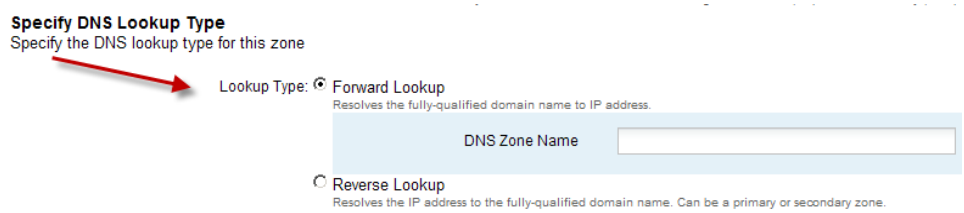
3.From the dropdown arrow, select a DNS server to apply the zone to.



4.Specify the **Zone Type**.

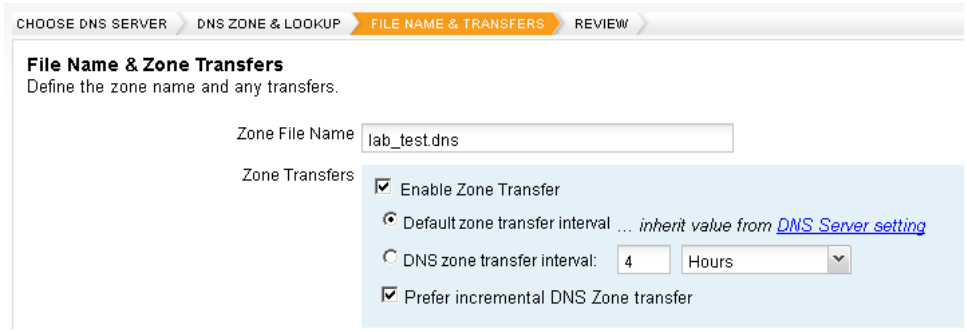


5.Specify the **DNS Lookup Type** and enter a **DNS Zone Name.**



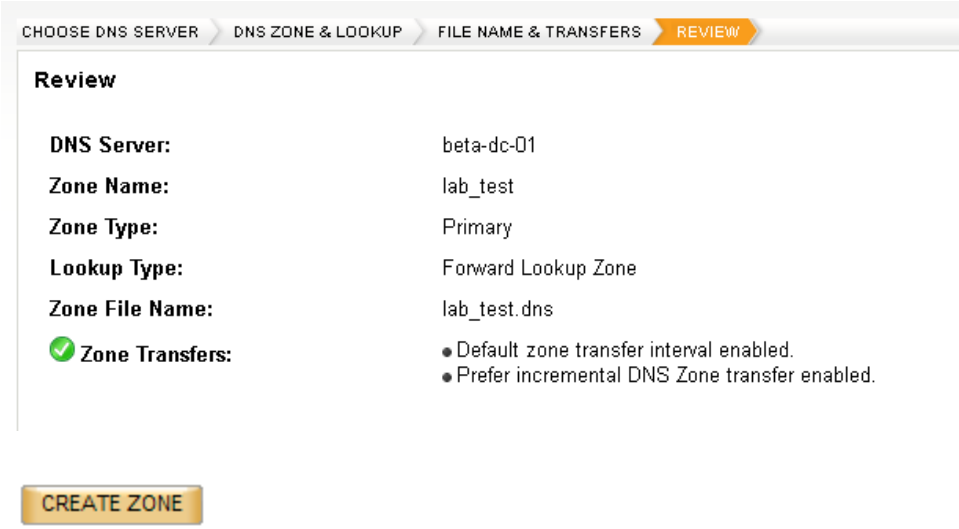
6.Click Next.

7.Specify the **Zone File Name** and select any transfers.

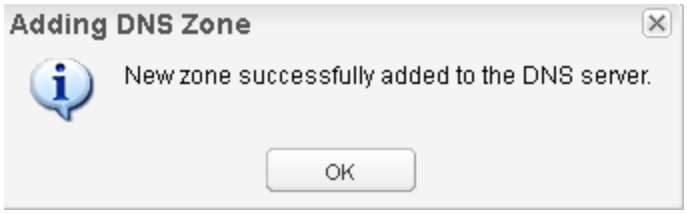


8.Click Next.

9.Review the information and click **Create Zone.**



10.Click **OK** on the confirmation.



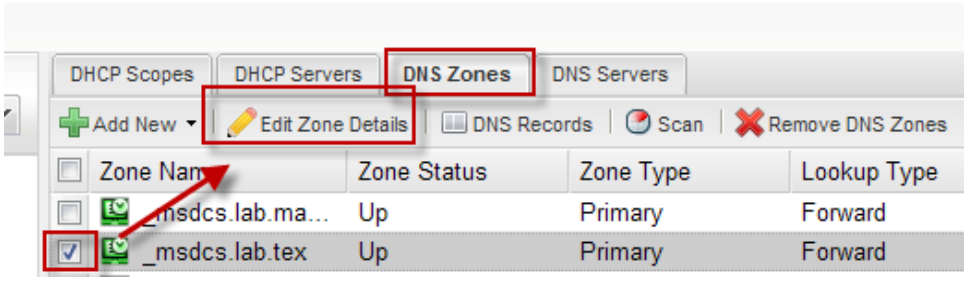
Editing a DNS Zone

To edit a DNS Zone-

1.Click the **DNS Zones** tab

2.Select a Zone to edit

3.Click **Edit Zone Details**

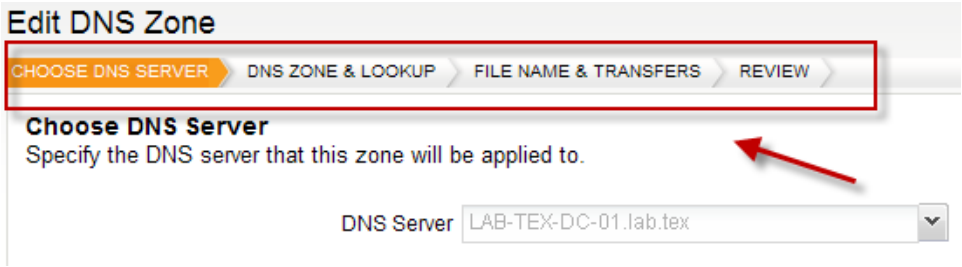


a.Edit the definition on the first tab of the wizard

b.Edit the Zone types and lookup types in the second tab of the wizard

c.DNS file name and zone transfer details in the third tab of the wizard

d.Review the details and click **Save**.



Bind DNS Monitoring & Management

IPAM offers support of (Linux based) BIND DNS Server monitoring and management.

BIND Credentials

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

IPAM supports BIND version 8 and higher, it is recommended to use BIND 9.1, as it supports commands for checking configuration syntax, which IPAM is able to use for configuration change validation during management operations.

Required Permissions

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: IPAM needs read and write access to the system temp directory /tmp CLI Commands: IPAM utilizes both standard Linux commands (POSIX) and BIND specific commands. This is the complete list of commands used by IPAM for both

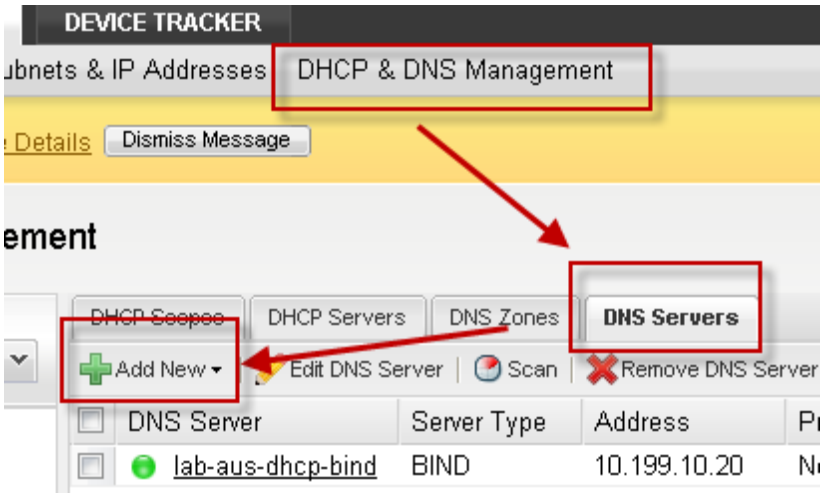
management and monitoring:

- 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

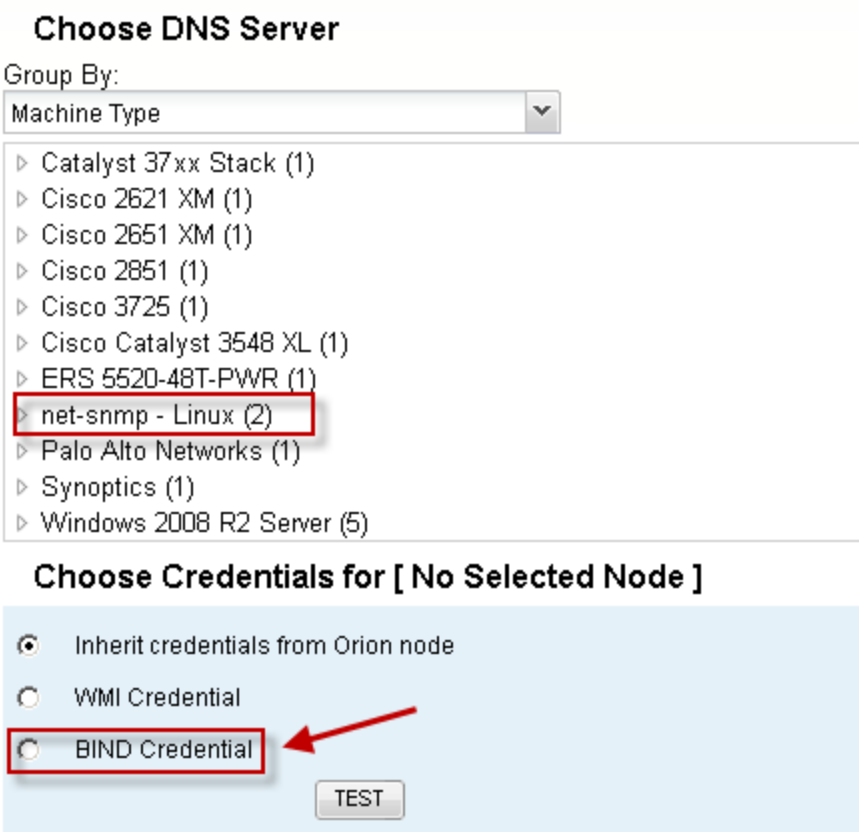
Adding a BIND to IPAM uses a simple wizard that guides you through the process. When added in IPAM, your device will sync and import actual BIND DNS configurations which can then be monitored or managed.

To add a BIND DNS Server:

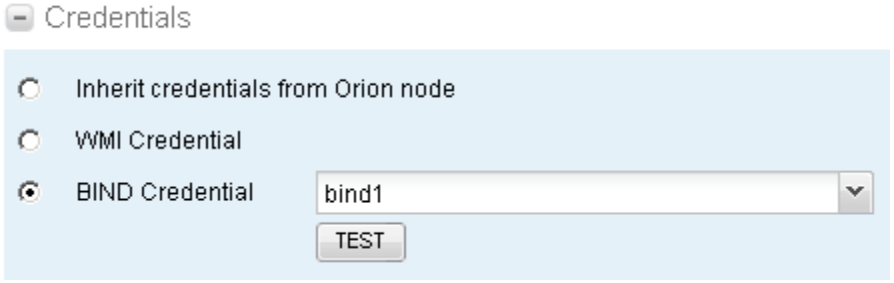
1.Click **DHCP & DNS Management > DNS Servers tab > Add New DNS Server.**



2.Select your BIND DNS Server from the populated list and then select BIND Credential. Create a new one if needed.



3.Enable scanning and then click **Add Server**.


Credentials
Inherit credentials from Orion node
WMI Credential
BIND Credential
bind1
TEST