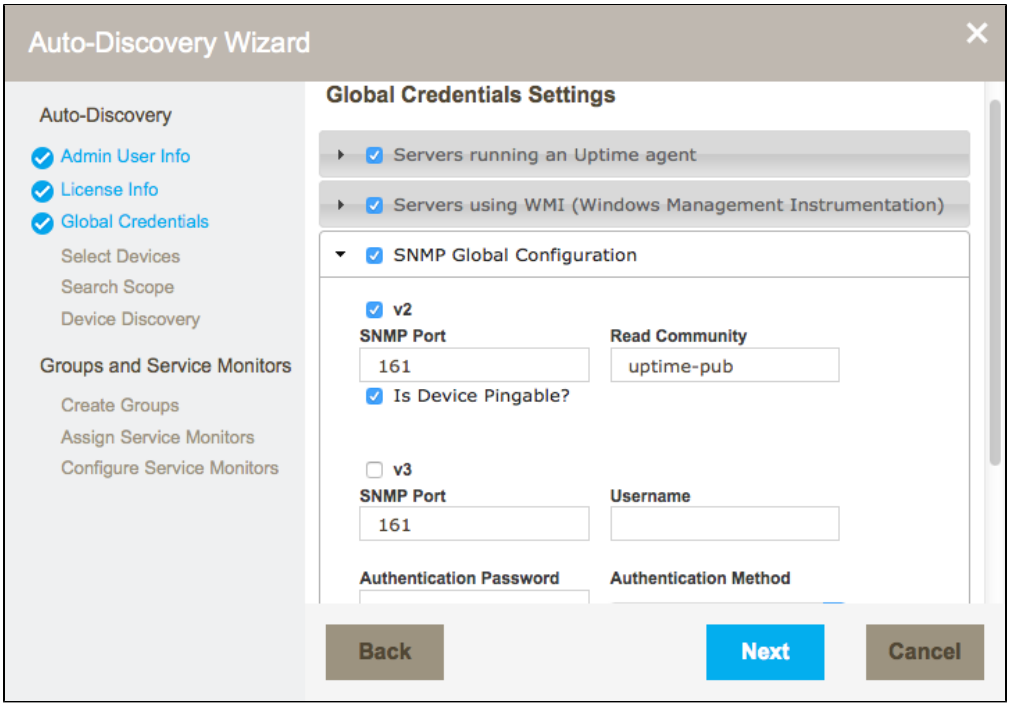
Using the Auto-Discovery Wizard

The Auto-Discovery wizard runs automatically the first time you launch Uptime Infrastructure Monitor or can be launched at any time by clicking the Config tab, and then clicking **Discovery Wizard** from the left menu. This wizard uses the same process of discovery as the existing Auto Discovery functionality but provides it through a wizard interface. Auto Discovery is still available in the Infrastructure tab. Note that buttons that include white text are active while buttons that include black text are inactive.

Set global credentials

The Global Credentials Settings page of the Auto-Discovery Wizard allows users to set global configurations and credentials including :

- Servers running an Uptime Agent
- Servers using WMI (Windows Management Instrumentation)
- SNMP Global Configuration (v2 and v3)

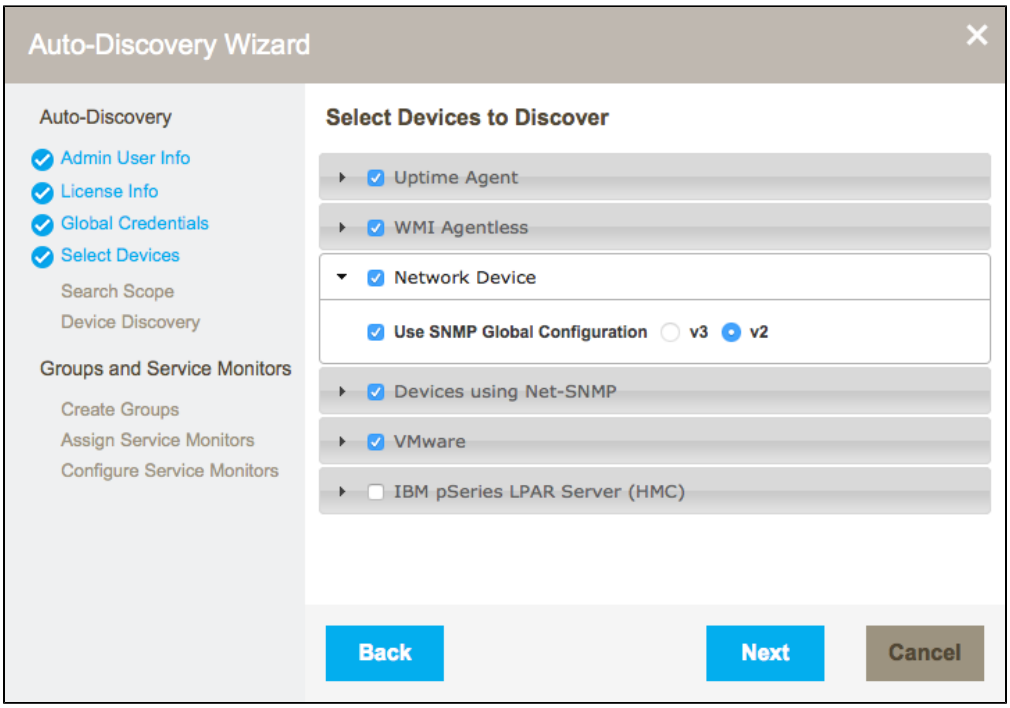


Select device types for discovery

The Auto-Discovery Wizard Select Devices to Discover page lets users set options to filter the types of devices discovered when the wizard runs. All of the following device types can be discovered and added in a single pass of the Auto-Discovery Wizard:

- Uptime agents
- WMI agentless
- Network devices
- Devices using Net-SNMP
- VMware
- IBM pSeries LPAR servers (HMC)

Note that when you choose an option, additional configuration options appear.



Auto Discovery for Servers and Network Devices

With Auto Discovery, Uptime Infrastructure Monitor can detect systems on your network that have an IP address within a specified range, as well as other search criteria:

- the `ping` utility is used to determine whether systems are available on the network
- an Agent check is performed to determine which systems have the Uptime Infrastructure Monitor Agent installed on them
- a WMI check is used to determine whether Windows-based systems are using WMI to gather performance metrics
- SNMP-based network devices are detected
- an SNMP probe is done to find any systems that are using Net-SNMP

Systems that are repeatedly discovered with different checks (e.g., both an Uptime Infrastructure Monitor Agent and WMI implementation are detected on the same system) are by default assigned a type based on the first check that resulted in its discovery. The auto-discovery order is as follows: agent check, WMI check, network device discovery, Net-SNMP probe.

Once a list of systems in the range of IP addresses that you specified is generated, you can selectively add them to Uptime Infrastructure Monitor.

Uptime Agents

Provide Uptime Infrastructure Monitor Agent connection information to allow the Monitoring Station to detect systems that have the Agent installed on them. Select the **Use Uptime Agent Global Configuration** check box if this information is configured (see Configuring Global Data Collection Methods for more information); otherwise complete the following options:

- **Agent Port Number**
  The port through which the Uptime Infrastructure Monitor Agents communicate with the Uptime Infrastructure Monitor Monitoring Station.
- **Use SSL (HTTPS)**
  Select this check box if the Agent securely communicates with the Monitoring Station using SSL.

WMI Agentless

Provide login information for an administrative Windows account if you would like Auto Discovery to scan for systems that are using WMI to collect metrics. Select the **Use WMI Global Configuration** check box if this information is configured (see Configuring Global Data Collection Methods); otherwise complete the following options:

- **Windows Domain** (optional)
  The Windows domain in which WMI is implemented.
- **Username**
  The name of the account with access to WMI on the Windows domain.
- **Password**
  The password for the account with access to WMI on the windows domain.

> This option is only available on Monitoring Stations running on the Windows platform.

Network Device

Provide connection information to allow Auto Discovery to scan for network devices. To comment to SNMP-based devices, select the **Use SNMP Global Configuration** check box, and then choose which version of SNMP is in use (see Global SNMP Configuration Settings); otherwise complete the configuration options as described in the next subject, "Devices using Net-SNMP."

Devices using Net-SNMP

Provide SNMP connection information to allow Auto Discovery to scan for servers with Net-SNMP. Select the **Use Global SNMP Configuration** check box if this information is configured (see Global SNMP Configuration Settings for more information); otherwise select the SNMP Version that your servers are using, then complete the appropriate options:

- **SNMP Port**
  The port on which the Net-SNMP instance is listening.
- **Read Community**
  A string that acts like a user ID or password, giving you access to the Net-SNMP instance. Common read communities are public (enables you to retrieve read-only information from the device) and private (enables you to access all information on the device).
- **Username**
  The name that is required to connect to the Net-SNMP instance.
- **Authentication Password**
  The password that is required to connect to the Net-SNMP instance.
- **Authentication Method** (optional)
  From the list, select one of the following options which determines how encrypted information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor is authenticated:
  MD5: A widely-used method for creating digital signatures used to authenticate and verify the integrity of data.
  SHA: A secure method of creating digital signatures. SHA is considered the successor of MD5 and is widely used with network and Internet data transfer protocols.
- **Privacy Password**
  The password that you want to use to encrypt information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor.
- **Privacy Type** (optional)
  From the list, select one of the following options that determines how information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor is encrypted:
  DES: An older method used to encrypt information.
  AES: The successor to DES, which is used with a variety of software that require encryption including SSL servers.

> You can set both the authentication method and password types, only one of them, or neither.

- **Is Device Pingable?** (appears only when using the **Network Device** option)
  Check this box if you can use a ping to verify the status of this device.

Auto Discovery for VMware vCenter Inventories

A VMware vCenter server acts as a central control point for a VMware vSphere datacenter. It includes ESX hosts, VMs, as well as groupings such as clusters, datacenters, vApps, and resource pools. A VMware vCenter server's inventory, system configurations, storage profiles, and performance data can be represented in Uptime Infrastructure Monitor alongside physical systems and network devices. When a VMware vCenter is added, all of its resources are detected and can be automatically imported.

VMware

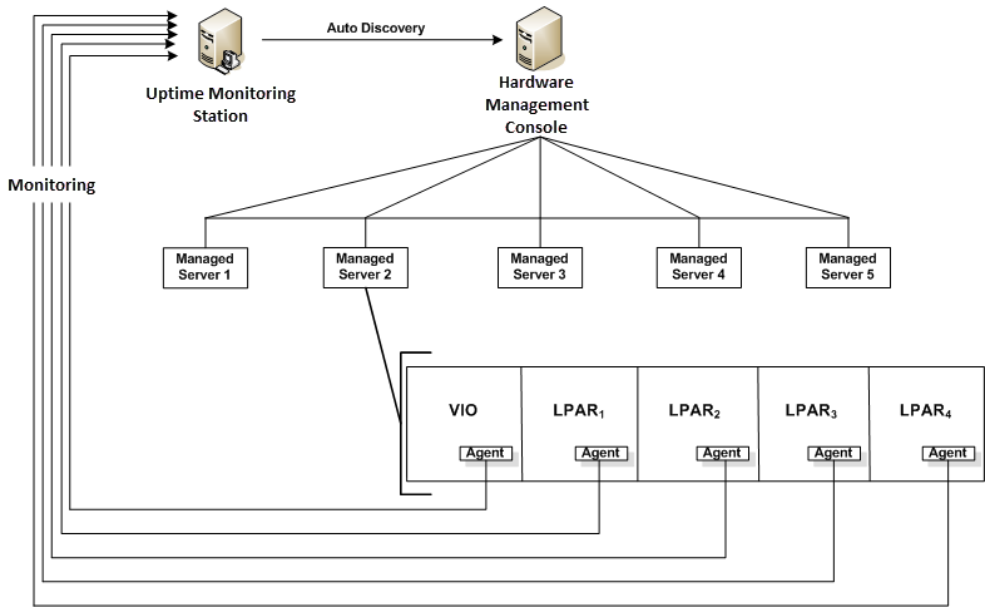
Provide VMware vCenter connection information to allow Auto Discovery to import its resources by completing the appropriate options:

- **Web Services Port**
  Accept or modify the default port through which Uptime Infrastructure Monitor connects to the server.
- **Username** and **Password**
  Login credentials for the VMware vCenter administrator.
- **Group**
  The group into which newly-discovered data is placed.

IBM pSeries LPAR Server (HMC)

You can also use the Auto-Discovery Wizard to add pSeries systems that are managed by the Hardware Management Console (HMC). The HMC is an interface for managing and configuring pSeries servers that are hosting multiple logical partitions (LPARs). When an HMC is attached to one or more pSeries servers with LPARs, the servers are considered managed servers.

In this configuration, the HMC manages all I/O requests from the LPARs. Use the Auto Discovery feature to detect the managed servers and add them to Uptime Infrastructure Monitor. Through the HMC, Uptime Infrastructure Monitor polls the agents installed on the VIO and the LPARs on a pSeries server for workload and other data, as illustrated below:



In order to monitor the managed servers and their LPARs, Uptime Infrastructure Monitor must communicate with the HMC.

> Before Uptime Infrastructure Monitor can communicate with an HMC, you must enable SSH on the latter. See the Uptime Knowledge Base article entitled *Enabling SSH on the Hardware Management Console* for more information.

Provide HMC-Managed pSeries server connection information to allow Auto Discovery to find devices by completing the appropriate options:

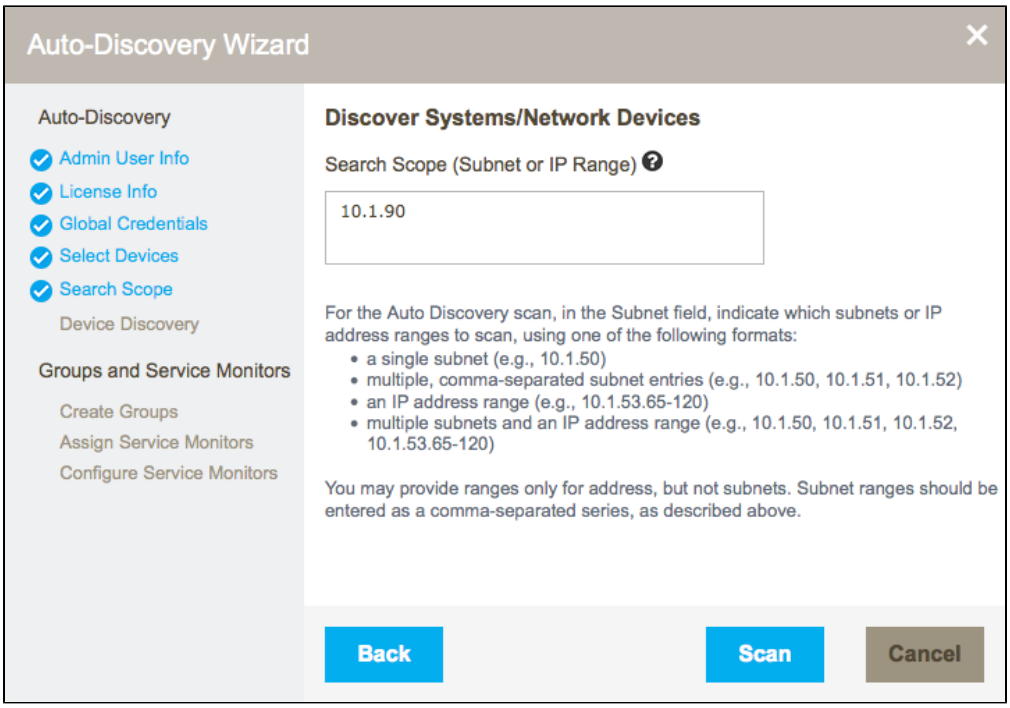
- **Hostname**
  The name of the system on which the HMC is running.
- **Username** and **Password**
  The credentials required to log into the HMC.

Set the search scope

Restrict the range the Auto-Discovery Wizard searches using the Discover Systems/Network Devices page. Indicate which subnets or IP address ranges to scan, using one of the following formats:

- a single subnet (e.g., 10.1.50)
- multiple, comma-separated subnet entries (e.g., 10.1.50, 10.1.51, 10.1.52)
- an IP address range (e.g., 10.1.53.65-120)
- multiple subnets and an IP address range (e.g., 10.1.50, 10.1.51, 10.1.52, 10.1.53.65-120)

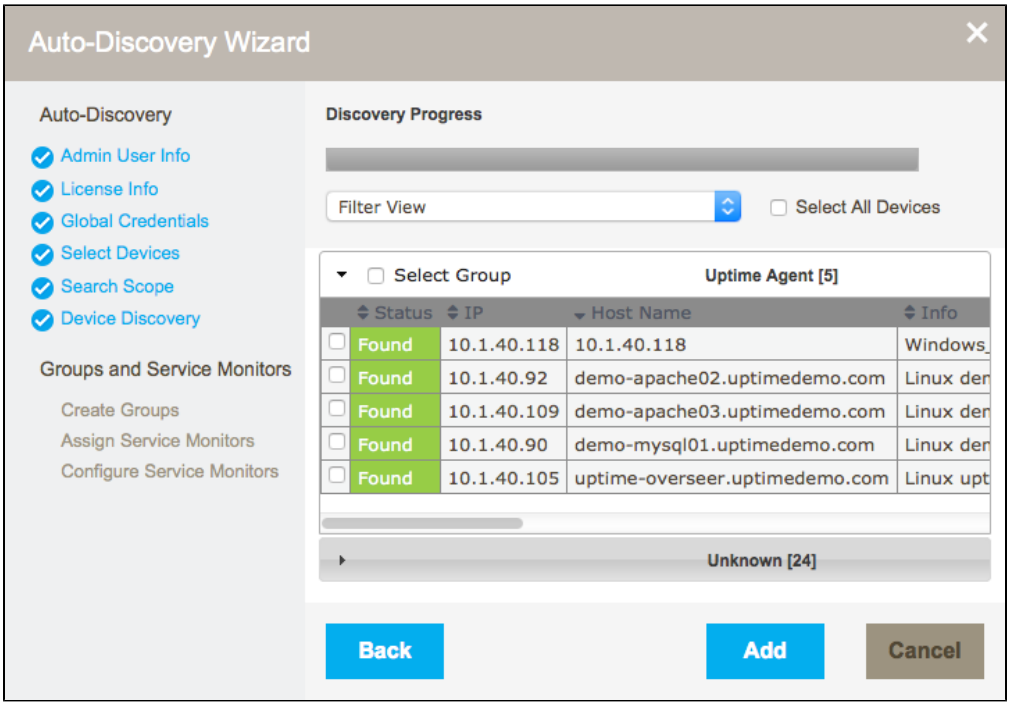
> You may provide ranges only for address, but not subnets. Subnet ranges should be entered as a comma-separated series, as described above.



Using discovered devices

Once discovered, select devices to:

- create groups
- add Service Monitors
- configure Service Monitors



Create groups

Depending on the type of devices added, Uptime Infrastructure Monitor automatically creates the following device groups:

- Windows Servers
- Linux Servers
- VMware

- IBM Servers

The Auto-Discovery Wizard also automatically creates the following groups, which can be viewed in the Infrastructure tab:

- Applications
- SLA

Add Service Monitors

Easily add service monitors to devices found and added in discovery. Default values allow users to simply review, and then click **Next** on the parameter steps to add the monitors. In addition to the monitors created by default, users can easily add:

- Windows servers added:
  - Windows Server Performance
    - Performance Check
    - File System Capacity
  - MS-SQL Checks
    - Windows Service Check (MSSQLSERVER)
    - SQL Basic Check (runs a query to test query engine)
    - SQL Advanced Checks (pulls performance information from the DB engine)
  - Active Directory
    - Directory Services Test
    - DNS

- Linux servers added:
  - Linux Server Performance
  - Performance Check
  - File System Capacity

- Any servers added:
  - MySQL Checks
    - MySQL Basic Checks (runs a query to test query engine)
    - MySQL Advanced Checks (pulls performance information from the DB engine)