Add Physical Servers

Not planning to do this module? You can skip to the next one. However, even if you plan to monitor only your vCenter Server, there are some important concepts covered in this module that are as applicable to your instances as they are to physical servers. Even if you do not perform the steps in this module, consider following along to learn more about agent- and WMI-based data collection.

This module consists of the following exercises:

Exercise	Description	Time required
Install an Agent on a Server	Install an agent script on a server for enhanced metric collection.	1 slice
Configure Global Agent Collection	Configure Uptime Infrastructure Monitor to use a standard set of properties to add agent-based servers with Auto Discovery.	½ slice
Configure Global WMI Collection	Configure Uptime Infrastructure Monitor with details about your WMI implementation, to add Windows-based servers with Auto Discovery.	½ slice
Add Agent and WMI Servers Using Auto Discovery	Use Auto Discovery to detect different server platforms.	1 slice
Review Your Current Inventory	Review your discovered inventory so far. Learn how to view performance and system information for an Element.	1 slice

Install an Agent on a Server

watch out!

Although there are Uptime Infrastructure Monitor agents for various platforms including Linux, UNIX, and Windows, in this module, you can install an agent on a Linux server.

Although agents are installed, they require minimal configuration and management, and have a small resource footprint. They are a low-cost way to get more detailed metrics from, and greater control over, a monitored system. For example, a VM that is part of a Hyper-V host or vCenter Server can be monitored based on the metrics provided by that server; however, an agent allows you to see what is happening at the service/application level.

Prerequisites

- you have identified on which test Linux server you want to install the agent
- an RPM utility is installed (and is in path) on the test Linux server
- xinetd is installed on the test Linux server
- you have downloaded the agent for this platform (`uptimeagent-6.0.0-linux-x86_64.rpm`), and transferred it to the server

1. Log into the system as user root.
2. Run the following command:
   `rpm -i uptimeagent-6.0.0-linux-x86_64.rpm`
   The agent install process performs various steps, such as restarting `xinetd`, and verifying dependencies such as `netstat` and `vmstat` exist.
3. Confirm via the command-line feedback that the installation is complete.

Pro Tip

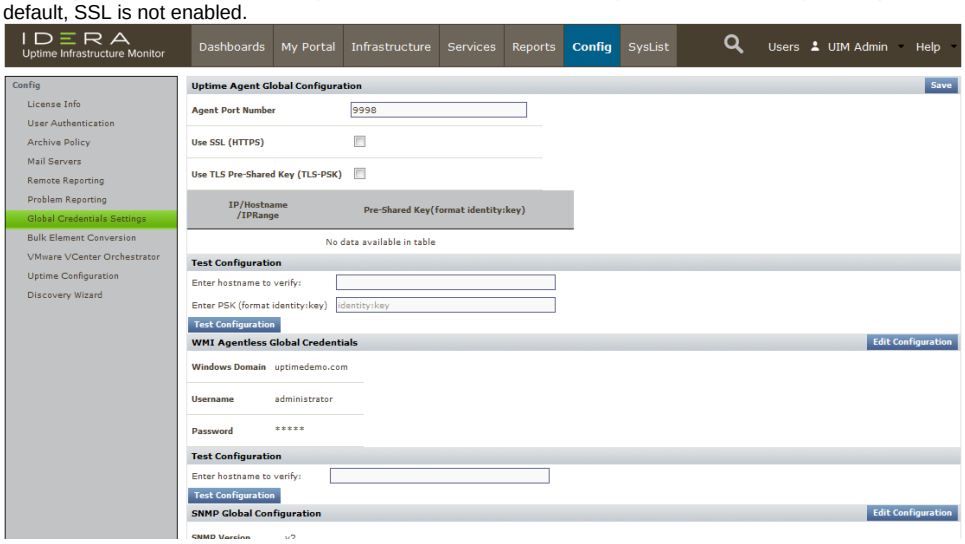
Although this procedure was very hands-on, naturally for an actual, large-scale deployment, you can consider a deployment solution such as Puppet, or BigFix for Windows agent installations.

Configure Global Agent Collection

Now that you have installed an agent on a server, you could add it to Uptime Infrastructure Monitor by using its host name. However, in a more realistic deployment, you would likely be installing agents on many servers. In this scenario, using Auto Discovery can expedite the process if you tell Uptime Infrastructure Monitor how to find all servers with an agent installed.

1. In the Uptime Infrastructure Monitor Web interface, begin by clicking **Config**, then click **Global Credentials Settings** in the left pane.
   On this page are configuration fields that let you define properties of different metric collection methods, allowing you to automatically discover large groups that share the same properties.

2. In the **Uptime Agent Global Configuration** section, click **Edit Configuration** on the far right. The port used to communicate with is 9998. By default, SSL is not enabled.



3. Click **Save**.

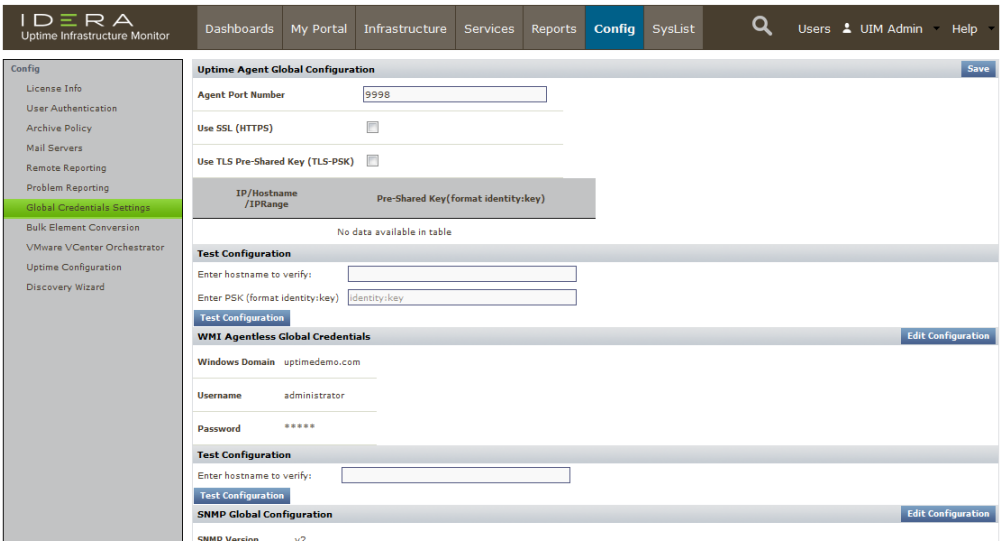
Validation Step: Test the global setting by entering the hostname of the Linux server you installed the agent on during the previous exercise, and then clicking **Test Configuration**.

This Linux server is now ready to be added to Uptime Infrastructure Monitor as an agent-based Element. Before doing this, let's take a look at how enhanced metrics can similarly be collected for Windows-based servers.

Configure Global WMI Collection

As an alternative to the Windows Uptime Infrastructure Monitor agent, Windows Management Instrumentation can provide deeper metrics for Uptime Infrastructure Monitor that is similar with agent-based data collection. The advantage is that it makes use of your existing infrastructure, negating the need for agent deployment. All you need to do is provide the WMI administrator information to the Uptime Infrastructure Monitor Monitoring Station, so that it is able to access Windows-based servers.

As with global agent settings, the **WMI Agentless Global Credentials** section of the **Global Credentials Settings** page lets you input WMI information once at a central point:



Configure the settings similar to those shown above:

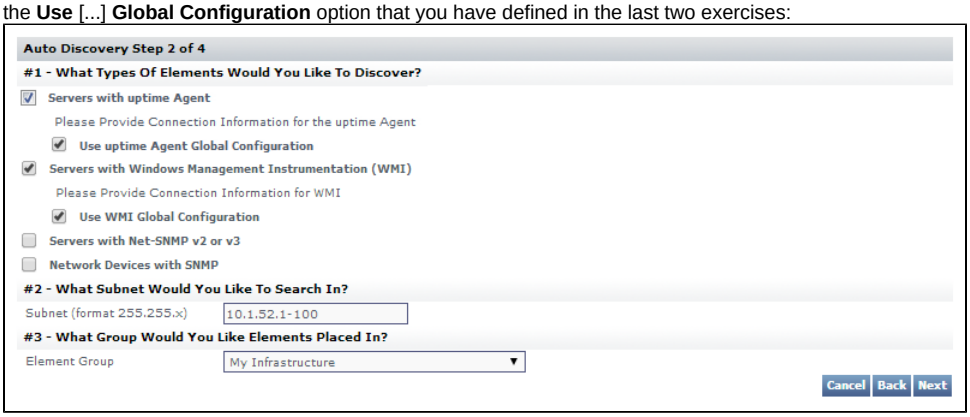
- **Windows Domain**: The Windows domain in which WMI is implemented.
- **Username**: The name of the account with access to WMI on the Windows domain.
- **Password**: The password for the account with access to WMI on the windows domain.

Validation Step: Test the global setting by entering a Windows host that the Monitoring Station can see in the **Test Configuration** section.

You are now ready to find an agent-based Linux server, and WMI Windows server.

Add Agent and WMI Servers Using Auto Discovery

1. Click **Infrastructure**, then click **Auto Discovery** in the left pane.
2. In the **Auto Discovery** pop-up, confirm that the selection is **Discover Servers and Network Devices on your network**, and click **Next**.
3. In the next step, select **Servers with Uptime Agent**, and **Servers with Windows Management Instrumentation (WMI)**. In both cases, select the **Use** [...] **Global Configuration** option that you have defined in the last two exercises:

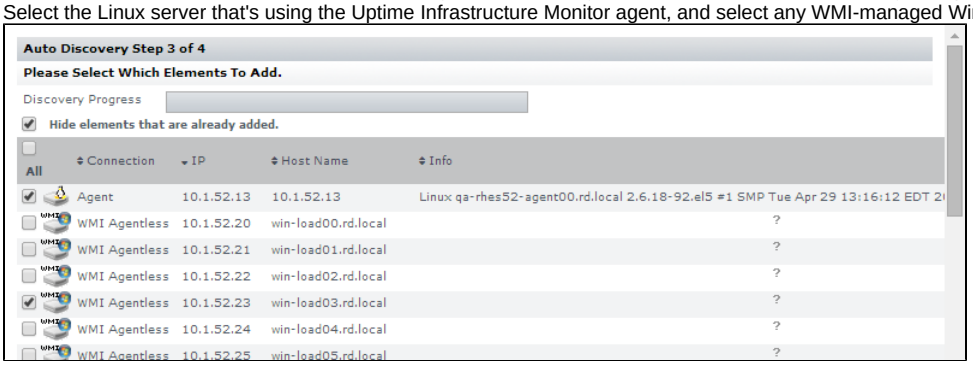


4. Enter the subnet or IP address range, similar to above.

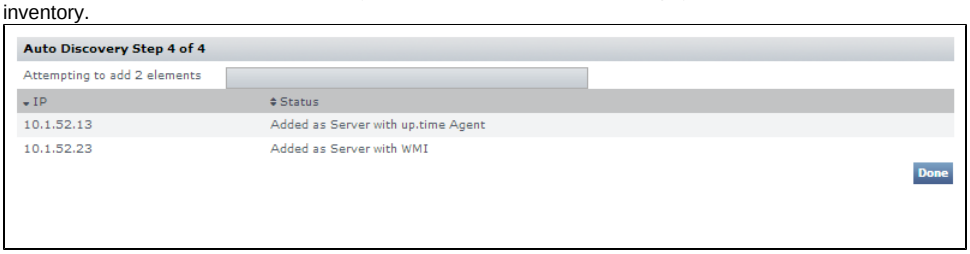
> **Pro Tip**
>
> Although we are keeping things simple, and using a single subnet or IP address range as shown above, there are other ways to point Uptime Infrastructure Monitor at subnets and subnet ranges to expedite the Auto-Discovery process. See Using Auto Discovery for more information.

5. Click **Next** to start the **Auto-Discovery** process.

6. When all servers on the subnet or IP address range are detected, you can make selections to add to your Uptime Infrastructure Monitor inventory. Select the Linux server that's using the Uptime Infrastructure Monitor agent, and select any WMI-managed Windows server.



7. Scroll to the bottom of the Auto Discovery list, and click **Add**. As a final step, you receive confirmation that these are now part of your monitored inventory.



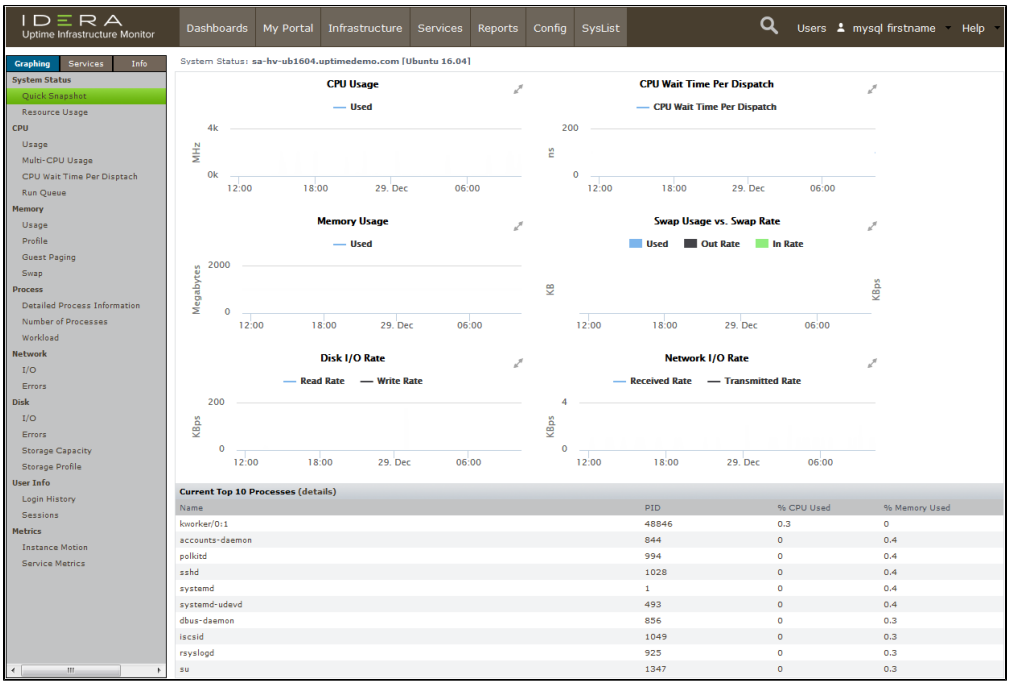
8. Click **Done**.

Review Your Current Inventory

After adding servers and closing the **Auto Discovery** window in the previous exercise, the main Uptime Infrastructure Monitor UI window is at the **Infrastructure** view. Refresh the page (or click **Infrastructure**) to ensure the latest additions appear immediately.

If you followed the Hyper-V or vCenter Server track, your inventory already included the virtual server Element and Infrastructure Groups created over those exercises. In addition, you now see the Linux server and WMI-managed Windows server you added in the previous exercise. Your inventory is now a mixed virtual-physical, multi-platform mix (although a small one). Also note the platform-specific icons beside each Element type.

Validation Step: Click a newly added server's gear icon. Then in the pop-up menu, click **Graph Performance** to go to its **Quick Snapshot**.



In the VMware vCenter Server track, you viewed Quick Snapshots for the vCenter Server element, and a VM-type Element. Compared to the latter, the Quick Snapshot for an agent- or WMI-based server includes more detail, such as process information, which can be acted upon by Uptime Infrastructure Monitor (for example, Uptime Infrastructure Monitor's action scripts can restart a service as a follow-up remedy to an outage).

Because performance metrics are gathered in real time by the Uptime Infrastructure Monitor agent or via WMI, there is nothing yet to display in the Quick Snapshot graphs. After moving through more of this Getting Started Guide, return to this Quick Snapshot to view some data.

> **License Check!**
>
> Verify how many license spots are free by clicking **Config,** then clicking **License Info** in the left pane. The number of used licenses is displayed in the **License Information** section.
>
> In this Getting Started Guide, the next track has you adding network devices. If you plan on following this track, you need to anticipate the number of network devices you plan to add. At minimum, you'll need at least 1.
>
> If you have run out of license spots, it's likely you have added a Hyper-V or vCenter Server. The easiest way to free up space is to manually ignore VMs; each VM you ignore opens a license spot for a new Element. Return to the Inventory Detail view for the Hyper-V/vCenter Element (**Infrastructure** > gear icon > **View** > **Inventory Detail**). Select VMs, ESX hosts, or even an entire cluster, then click **Add Selected Elements to Ignore**. The spots are freed up in your license, which you can verify by clicking **Config** > **License Info**.

Back: Add a VMware vCenter Server

Next: Add a Network Device