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.

Using Auto Discovery

To use Auto Discovery for systems and network devices, do the following:

1. In the **Infrastructure** panel, click **Auto Discovery**.
   The **Auto Discovery** window appears.
2. Ensure Auto Discovery is set to **Discover Servers and Network Devices on your network**, and then click **Next**.
3. Select one or more types of network entities to include in the auto-discovery process:
   - Servers with Uptime Agent
   - Servers with Windows Management Instrumentation (WMI)
   - Servers with Net-SNMP v2 or v3
   - Network devices with SNMP

   With each selection, additional configuration options appear.
4. Optionally 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:
   - **Port**
     The port through which the Uptime Infrastructure Monitor Agents communicate with the Uptime Infrastructure Monitor Monitoring Station.
   - **Use SSL**
     Select this check box if the Agent securely communicates with the Monitoring Station using SSL.
   - **Use PSK**
     Select this check box if the Agent securely communicates with the Monitoring Station using Pre-Shared Key (PSK) authentication.
5. Optionally 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 available only on Monitoring Stations running on the Windows platform.

6. Optionally provide SNMP connection information to allow Auto Discovery to scan for servers with Net-SNMP. Select the **Use Global SNMP Connection 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 Version**
     The version of SNMP in use.
   - **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.

7. Optionally provide SNMP connection information to allow Auto Discovery to scan for SNMP-based network devices. Select the **Use Global SNMP Connection Configuration** check box if this information is configured (see Global SNMP Configuration Settings); otherwise complete the configuration options as described in the previous step.
8. For the Auto Discovery scan, in the **Subnet** field, 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.

9. Select the **Element Group** in which these additions are placed.
10. Click **Next** to begin the auto-discovery process.
    A list of the systems that match all your defined criteria is generated. The time required for the list to populate is dependent on the breadth of your search criteria.
11. When the auto-discovery list is completed, select the corresponding check boxes for all the network entities you wish to add to Uptime Infrastructure Monitor as monitored Elements.
12. Click **Next** to begin adding your selections.
    As your selections are added to Uptime Infrastructure Monitor as Elements, the progress of their addition is displayed.

> If this process is not fully completed, none of the queued network entities become Uptime Infrastructure Monitor Elements.

13. Click **Done**.
    All of the new Elements appear in the selected Element group under **Infrastructure**.