Discovery

What does "Discovery" in Unimus mean?

To make device management easier and to automate bulk operations, Unimus uses a discovery mechanism. Thanks to discovery, you do NOT need to give Unimus precise information about every device in the system (such as username/password, vendor, device type, model, etc.). Unimus will be able to discover all of the details about your devices automatically. This heavily decreases workload when deploying Unimus to your network, as all Unimus needs are IP addresses of your devices, nothing else. In other words, you can import 100 devices into Unimus using our Address import feature, and they will all start working properly, instead of having to manually configure the details for each device.

What happens during Discovery?

The discovery mechanism works in stages:

Detect available connector

All available ports for all enabled connectors are checked. More info in Connectors and ports.

Secure connectors are always preferred to insecure connectors.
For example, if a device is available over both Telnet and SSH, SSH will be used.

Detect credentials

Credential discovery works differently depending if the device is set to "Discover" credentials, or has "Bound" credentials.

If credential discovery enabled:
All credentials configured in the 'Credentials' settings are checked against the device.
Credentials are checked against the device in random order.

Whichever credentials work on the device first will be used for any future operations with this device.

When credentials bound to device:
Only bound credentials are tested against the device
If bound credentials do not work, the job fails

Detect device vendor and model

After correct connector and credentials are known, Unimus discovers the device.

The Vendor, Type and Model of the device is discovered.

Detect available CLI modes on the device

After Unimus knows exactly which device it's working with, it discovers available CLI modes (enable / configure mode - for example "privileged exec" and "configure" on Cisco).

Device connections during discovery

Unimus can open multiple connections to a device during discovery. How many sessions are opened depends on how many credentials are available for a device.

If a single credential is available for a device

If only a single credential is available for a device (when using Credential Binding, or Discovery with only a single credential added in the "Credentials" screen), Unimus will only open a single CLI session to the device after finding an available connector. Unimus will open connections to multiple devices at the same time (this can be configured as per the Changing maximum job concurrency article), but there will only be a single connection to each of these devices.

Assuming only a single connector is defined, and a single credential is available for a device, Unimus will open:

- 1x TCP session to the device to check if SSH/Telnet is available (a TCP 3-way handshake will be performed and then the TCP session will be closed)
- 1x full CLI session will be negotiated (SSH/Telnet as configured by Connectors) and will be used to detect device vendor, model CLI modes, etc.

Please note this behavior applies to versions 2.2.0 and newer. Older Unimus versions will behave as described in the section below, even when only a single credential is available.

If multiple credentials are available for a device

If a device is set for credential discovery and multiple credentials are available, it is normal (and expected) for Unimus to open multiple successive SSH (or Telnet) sessions to a single device during Discovery. Please note multiple concurrent sessions will never be opened to a single device, only a single session will be opened at one time to any particular device. Unimus will open connections to multiple devices at the same time, this can be configured as per the Changing maximum job concurrency article.

Unimus will open 2 + [number of available credentials] SSH (and/or Telnet) sessions to each device during Discovery:

- 1x session to check if the connector is available (during Connector detection)
- 1x session per available credential (during Credential detection)
- 1 final session which will be used to detect device vendor, model CLI modes, etc.

To minimize the number of SSH/Telnet sessions made to devices during Discovery, please use credential binding, as described in the above section of this article.

Adjusting Discovery performance

As per the previous section, you can adjust the maximum number of Discovery jobs in the job concurrency settings to throttle down the maximum number of concurrently running jobs. This will generate less peak outbound SSH/Telnet sessions from Unimus, and spread them over a longer period. You can also adjust the "unimus.core.inter-connection-delay" setting in timeouts configuration to slow down the rate of logins to individual devices, in effect lessening the speed of outbound SSH/Telnet sessions to each individual device.

When is Discovery performed?

Device addition into the system

The discovery mechanism is what makes only the address of the device required when adding a new device into Unimus.
Unimus will automatically discover everything else about the device.

Import

When 400 devices are imported into Unimus, Unimus will automatically discover all the necessary details about each of the devices, and start backing them up automatically.
If proper connectors and credentials are configured, no additional steps other than importing the devices are needed.

This saves time for the administrators, and automates the work-flow.

Scheduled backups

Unimus performs a discovery before each scheduled backup.
This is to make sure Unimus knows current information about the device (connector, credentials, vendor, model, etc.).

The discovery before backup is necessary to make sure Unimus doesn't use wrong commands on the device.
In certain situations (ex. when a device is changed for another device) it's possible commands to generate backups on some vendors can actually cause configuration changes for other vendors.
Due to this (and other edge-cases) Unimus does a discovery before every backup.

Credential changes

Discovery mechanism will also be used if any device operation fails.
For example, if credentials which were previously used on a device are no longer valid on that device, Unimus will re-run discovery.

This means that if credentials used on 400 devices need to be changed, the only change needed in Unimus is to reconfigure the credentials in 'Credentials' settings.
Discovery mechanism will take care of the rest.

Device hardware changes

Discovery will automatically be re-run when device hardware change is detected.
For example, when a Cisco device is replaced with a MikroTik, or a HP device with an UBNT device, Unimus will handle this automatically.

This means that if devices are changed around the network, Unimus will automatically adjust to the situation, without the need for user interaction.

How to find out why device didn't discover?

There are 2 places in Unimus where you can see why discovery failed.

- Dashboard > Latest failed jobs
  You can select the discovery job, and press 'Show log'.

- Logs
  '/var/log/unimus' or 'C:\ProgramData\Unimus\log'

If you can't identify why you device didn't discover properly from either of these, feel free to contact support.
We will always be happy to help with any issues.