CONNECTWISE

Configuring Probe Templates

Overview

This page walks you through the process of accessing probe templates and conducting an SNMP walk.

Access the Probe Templates

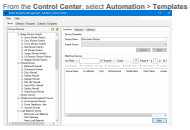
After the probe has been enabled (refer to the Network Probe documentation on how to enable the probe) and the basic configuration has been completed, further advanced configuration is available through detection and collection templates. These templates dictate how the probe discovers and interfaces with SNMP-enabled devices on the network. The Probe Templates allow you to classify the devices that the probe finds and also define what information it should collect from these devices.

The Probe Templates have three sections (tabs):

- **Library**: The Library tab displays all known devices in the device library, as well as the detection and collection templates that pertain to those devices. It allows the user to view the templates as they are used by the system.
- **Detection Templates**: The Detection Templates tab allows the user to review all detection templates.
- **Collection Templates**: The Collection Templates tab allows the user to review all collection templates. From here users can create custom templates that can be applied to individual devices.

To access the Probe Templates, follow the steps listed below:

1. From the **Control Center**, select **Automation** > **Templates** > **Probe Templates**.



All discovered devices since the probe was first initiated display in the **Matching Devices** section of the **Inventory** tab (default).

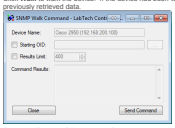
Conduct an SNMP Walk

The SNMP Walk command essentially performs a series of GETNEXT commands and stops when it returns results that are no longer inside the range of the OID that you originally specified. You can use the SNMP Explorer to evaluate the information provided by a device and create collection templates based on the information you find during the walk.

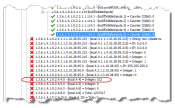
This section of the document walks you through doing an SNMP Walk and downloading a MIB file to correct missing OIDs.

1. To walk a device from the **Control Center** click **Browse** > **Clients** > **Network Devices** and then double-click on the device.
2. Click on the **SNMP Explorer** tab.

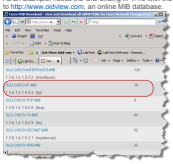
3. Select the **View As:** List or Tree option based on your viewing preference.
4. Select the **Separate Missing Results** checkbox if you want the OIDs with no corresponding MIB information at the bottom of the list/tree as opposed to where they logically fit in the tree.
5. Select the **Results Since** checkbox and select a date if you want to limit the data from a specific date.
6. Click **Walk** to walk the device. If the device had been walked before, you can click on **Refresh** to show the previously retrieved data.



7. Select the **Starting OID** checkbox if you want to start at a specific OID or you can click on the **Ellipsis** to select a starting OID from the **OID Selector**.
8. Select the **Results Limit** and enter the desired limit if you want to limit the results to a certain amount of data.
9. Click **Send Command** to start the walk.



A review of the walk data shows some OIDs have no information (indicated by the red x). These OIDs cannot be mapped to any OIDs from the known MIBs. However, there are online resources to download MIB files. The next few steps show you how.
As an example, notice the OID ending in 4.4.0 with the value 512. Doing a Google search leads us to http://www.oidview.com, an online MIB database.



10. As an example, download the *OLD-CISCO-IP-MIB* file and place it in the *LTShare\MIBS\RFC* directory.
11. Delete the *MibCacheDataSet.xml* file. This forces the **Control Center** to reload. Restart the **Control Center**. The status window shows that the MIBs were loaded successfully:

Now, if you look at the walk data, you can see that the highlighted OID is the 'Threshold of IP accounting records in use before IP traffic will be accounted'. This is probably not very useful; however, actLostPkts and actLostByts could provide valuable information.

- actLostPkts = Lost IP packets due to memory limitations.
- actLostByts = Total bytes of lost IP packets.
  Both values are 0. At this point, you could create a collection template for this data. Please note that when you are creating collection templates based on information received from a walk, that the data may be available to all known devices for a specific make of device (e.g., all Cisco known devices) and thus should be applied to the base object and not a specific model.
  Tip: Please note the units of the returned value when creating reports and monitors. It is common practice to return decimal values as integers offset by a power of 10 or 100. For example, a UPS may report a 5.6% battery power left as 56 or 560. So writing a monitor to find failing UPS devices (less than 10%) requires a SQL statement of "percent < 100" – not "percent < 10".