CONNECTWISE

Detection Templates

Overview

The Detection Templates tab lists all of the current detection templates that currently exist in the system. Selecting a template from the template listing displays all of the properties for that selected template. This is the same information that you would see in the Detection tab of the Library.

There are two types of detection templates that can be created in ConnectWise Automate®. Each of these use a distinct type of protocol:

- **SNMP**: SNMP detection templates allow for the detection of specific devices responding to an SNMP query as defined on the detection template.
- **SSDP**: SSDP detection templates send out an SSDP broadcast on port 1900 to evaluate any responding devices based on the criteria of the detection template.

In this article, learn how to:

- Add SNMP Detection Templates
- Add SSDP Detection Templates
- Modify Detection Templates
- Delete Detection Templates

Add Detection Templates

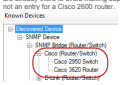
Detection templates should be added when a particular device has been identified that is not in the Automate Known Devices library AND you want to be able to retrieve information specific to that device or for reporting/ integration purposes.

As an example, let's walk through the process of creating a detection template for a Cisco 2600 router. This assumes you have already walked the device. For additional information on walking devices, please refer to Walking SNMP Devices.

Add SNMP Detection Template

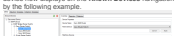
To add a new SNMP detection template:

1. Prior to adding a detection template, look at the **Known Devices** in the **Library** to see if the make and model are already there to avoid making duplicate templates. As you can see from the following example, there is not an entry for a Cisco 2600 router.



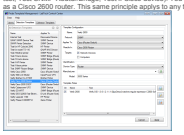
2. Click on the **Add**

icon. The **Device Properties** clears any existing data to allow you to enter the device information.
3. Enter the **Device Name** (e.g., Cisco 2600 Router).
4. Select the **Parent Device** from the drop-down menu (e.g., Cisco (Router/Switch) and click **Apply**. The device now displays on the **Known Devices** navigation tree under the parent device you selected as shown by the following example.



5. The next step is to add a detection template for this device. Click on the **Detection Templates** tab.
6. Click on the **Add**

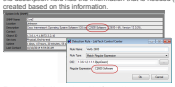
icon. This enables the **Template Configuration**, **Identification** and **Template Rules** section to allow input. **Note:** Because there is a parent device (e.g., Cisco Router/Switch) that has templates already created to identify it is a Cisco device, you do not need to recreate each detection template (e.g., templates: Internal test, Test SNMP Router/Bridge, Test if Cisco device). You only need to create the template that identifies it as a Cisco 2600 router. This same principle applys to any templates you create.



7. Enter the template name in the **Name** field. This should be a descriptive name that indicates what the template is doing (e.g., Verify Cisco 2600).
Tip: It is recommended that you use the same naming standard for all of the templates. This makes it easier to locate a specific template at a later date.
8. The **Protocol** defaults to SNMP. Leave this at the default.
9. Select the device type from the **Applies to:** drop-down (e.g., Cisco (Router/Switch).
10. Select the value to make the unit, if the template succeeds from the **Results In:** drop-down. The values in this drop-down are the device names that appear under the parent device in the **Known Devices** section (e.g., Cisco 2600).
11. Select the **Network Devices** and/or **Computers** checkboxes, if applicable. Selecting **Network Devices** and not **Computers** tells the template to run against only networked devices, not on computers with agents trying to self-collect.
12. Select the **Device Type** and **Manufacturer** from the drop-downs, if necessary. For this example, it is not necessary because the device has already been identified as a router and the manufacturer is Cisco.
13. Enter the **Model** of the device (e.g., 2600 Series).

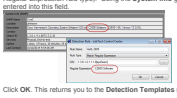
14. The next step is to create the rule. Click on the **Add Rule**

icon in the **Template Rules** section.
Because this device was walked previously to starting the creation of this template, it is already known that the description field has the information that is needed (as shown in the **System Info** below), so the rule is created based on this information.

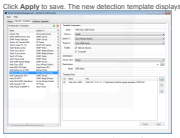


15. Enter the **Rule Name** (e.g., Verify 2600).
16. Select the desired **Rule Type** from the drop-down (e.g., Match Regular Expression).
    - **Run Internal Validation**: Runs a probe internal query that checks a particular OID or group of OIDs. The only internal query available at this time is Validates support for SNMPs. This runs a variety of SNMP Get commands to ensure device supports SNMP sufficiently for Probe requirements.
    - **Validate OID Exists**: The template queries the device for a particular OID. If the device responds to the OID (e.g., the OID is in it is MIB), then the rule will pass.
    - **Validate OID Does Not Exist**: The template queries the device for a particular OID. If the device does not respond to the OID (e.g., the OID is not in its MIB), then the rule will pass.
    - **Match Regular Expression**: The device is queried for the specified OID and the OID is compared to a regular expression. For the rule to pass the OID must exist and the resulting value must match the regular expression.
17. Enter the **OID** or click on the ellipsis to select the OID from the **OID Selector** as shown by the following example.

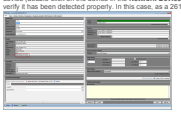
Note: For additional information in the OID Selector, refer to Use the OID Selector.
18. Once the correct OID is selected, click **OK** to accept. The **OID Selector** indicates that sysDesc – 1.3.6.1.2.1.1.1.0 is the textual description of the entity so this is selected for our example.
Note: The 0 in the above value indicates a single data value as opposed to a value in a table.
19. Enter the **Regular Expression** to match to the OID, if necessary (only available if you selected Match Regular Expression rule type). Using the **System Info** gathered from walking the sample device, C360-I-M is entered into this field.



20. Click **OK**. This returns you to the **Detection Templates** screen.
21. Click **Apply** to save. The new detection template displays on the **All Detection Templates** list.



22. Open the probe-enabled computer from the **Computer Management** screen of the Probe device, select **Begin** > **Commands** > **Probe** > **Refresh Configuration** to update the probe. The device will be detected during the next detection schedule or you may force the probe to re-detect by double-clicking the probe, selecting **Network Probe** > **General** and clicking **Re-Detect Devices**. You can check the network device (double-click on the device in the **Network Devices** tab on the **Clients** tab of the **Control Center**), to verify it has been detected properly. In this case, as a 2610 router as shown by the following example.

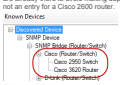


Add SSDP Detection Template

SSDP detection templates operate by sending out a broadcast across a network to discover devices that meet the criteria of the template.

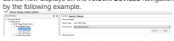
To add a new SSDP detection template:

1. Prior to adding a detection template, look at the **Known Devices** in the **Library** to see if the make and model are already there to avoid making duplicate templates. As you can see from the following example, there is not an entry for a Cisco 2600 router.



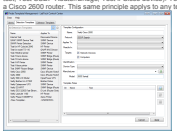
2. Click on the **Add**

icon. The **Device Properties** clears any existing data to allow you to enter the device information.
3. Enter the **Device Name** (e.g., Cisco 2600 Router).
4. Select the **Parent Device** from the drop-down menu (e.g., Cisco (Router/Switch) and click **Apply**. The device now displays on the **Known Devices** navigation tree under the parent device you selected as shown by the following example.



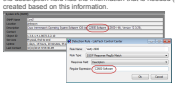
5. The next step is to add a detection template for this device. Click on the **Detection Templates** tab.
6. Click on the **Add**

icon. This enables the **Template Configuration**, **Identification** and **Template Rules** section to allow input. **Note:** Because there is a parent device (e.g., Cisco Router/Switch) that has templates already created to identify it is a Cisco device, you do not need to recreate each detection template (e.g., templates: Internal test, Test SSDP Router/Bridge, Test if Cisco device). You only need to create the template that identifies it as a Cisco 2600 router. This same principle applys to any templates you create.

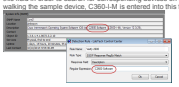


7. Enter the template name in the **Name** field. This should be a descriptive name that indicates what the template is doing (e.g., Verify Cisco 2610).
Tip: It is recommended that you use the same naming standard for all of the templates. This makes it easier to locate a specific template at a later date.
8. Select SSDP Search from the **Protocol** drop-down.
9. Select the device type from the **Applies to:** drop-down (e.g., Cisco (Router/Switch).
10. Select the value to make the unit, if the template succeeds from the **Results In:** drop-down. The values in this drop-down are the device names that appear under the parent device in the **Known Devices** section. For this example, the drop-down values consist of Cisco 2600 Router and Cisco 2610 Router. Because we are creating a template for the Cisco 2610 Router, that is the value to select.
11. Select the **Network Devices** and/or **Computers** checkboxes, if applicable. Selecting **Network Devices** and not **Computers** tells the template to run against only networked devices, not on computers with agents trying to self-collect.
12. Select the **Device Type** and **Manufacturer** from the drop-downs, if necessary. For this example, it is not necessary because the device has already been identified as a router and the manufacturer is Cisco.
13. Enter the **Model** of the device (e.g., 2600 Series).
14. The next step is to create the rule. Click on the **Add Rule**

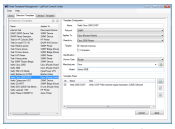
icon in the **Template Rules** section.
Because this device was walked previously to starting the creation of this template, it is already known that the description field has the information that is needed (as shown in the **System Info** below), so the rule is created based on this information.



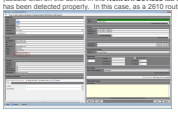
15. Enter the **Rule Name** (e.g., Verify 2600).
16. The default **Rule Type** is SSDP Response RegEx Match. The SSDP protocol only uses this rule type for the detection template.
17. Select the expected SSDP response (the type of information you expect to receive from the detected device; e.g., Description) from the **Response Field** drop-down.
18. Enter the **Regular Expression** to match to the SSDP Response Regex Match. A regex string is entered into this field in order to search for corresponding devices on the network. Using the **System Info** gathered from walking the sample device, C360-I-M is entered into this field.



19. Click **OK**. This returns you to the **Detection Templates** screen.
20. Click **Apply** to save. The new detection template displays on the **All Detection Templates** list.



21. Open the probe-enabled computer from the **Computer Management** screen of the probe device and select **Begin** > **Commands** > **Probe** > **Refresh Configuration** to update the probe. The device is detected during the next detection schedule or you may force the probe to re-detect by double-clicking the probe, selecting **Network Probe** > **General** and clicking **Re-Detect Devices**. You can check the network device (double-click on the device in the **Network Devices** tab of the **Clients** tab on the **Control Center**), to verify it has been detected properly. In this case, as a 2610 router as shown by the following example.



Modify Detection Templates

Great care should be taken when modifying detection templates because it could result in broken detection and collection sequences. If changes must be made, ensure that the detection templates are applied by refreshing the configuration for any locations that might contain devices that use the altered template.

1. From the **Detection Templates** tab, highlight the template to modify.
2. Make the necessary adjustments to the **Template Configuration** and **Identification** sections.
3. If any changes need to be made to the rules, select the rule and click the **Edit Selected Rule** icon. Make the necessary adjustments and click **OK**.
4. Click **Apply** to save the changes to the template.
5. Open the probe-enabled computer from the **Computer Management** screen and select **Begin** > **Commands** > **Probe** > **Refresh Configuration** to update the probe.

Delete Detection Templates

Great care should be taken when deleting detection templates because it could result in broken detection and collection sequences. If you decide to delete any detection templates, it also deletes any rules associated with the template.

1. From the **Detection Templates** tab, highlight the template to delete.
2. Click the

Delete icon.
3. You are prompted to confirm removal. Click **Yes** to remove the template and any associated rules or **No** to cancel.