CONNECTWISE

# Network Probe Tile

## Overview

A network probe is a service running on a designated computer in each location that will scan the network for other devices that do not have the ConnectWise Automate® agent installed on them, as well as network devices (e.g. routers and printers). The probe will scan the network when the service is started, then once a day (default setting). The probe can also be used to do a probe push to deploy agents. Enabling the Network Probe also enables SNMP Trapping, TFTP Server, and Syslog Event Trapping.

**Note**: Only Windows computers can be designated as network probes.

For any ports that may be used by the probe, all firewalls and antivirus software should be configured to allow traffic through those ports. This includes syslog port, SNMP trap listening port, and TFTP port. Automate enables you to customize and change listening ports on the fly. The probe does not automatically alter firewall settings.

**Important**: The probe push will fail if the following conditions are met: Antivirus software is set to block VBScripts, the Windows Firewall is enabled, any additional third-party firewall is enabled, or .NET version 4.0 or newer is not installed.

**Important**: A new network probe was released in ConnectWise Automate® v12. The Network Probe functionality documented in the Control Center articles refers to old network probes. For information on how new network probes operate, please refer to Network Probe Tile documentation. To upgrade to the new probe, select the Enable New Probe check box on the probe Overview Screen. Refer to Upgrading the Network Probe for instructions. If you enable a new probe, it functions as described in the Network Probe Tile documentation, even if you are using the Control Center.

## Probe Behavior

There are some limits to the probe. In order to not overwhelm the network or host machine, the probe is limited to 100 concurrent tasks. For example, during a network scan, if there are 30 IP Addresses to check, the probe will start with the first 15, and then as soon as one of the IP searches is complete, it will move to IP #16, then IP #17, and so on.

The probe polls every five minutes to see if a device is online or offline by means of a brief ping or port check to see if the devices are available. If the network is extremely busy, this may cause background scanning to temporarily fail, causing the probe to consider a device to be offline.

There are two basic types of network scans the probe can perform. The quick scan is a basic ping that pings the address to determine if it is available, while the full scan is more advanced and includes checking and validating SNMP information and ports. The type of scan performed will be indicated in the probe events log.

Once per day, the probe purges the network devices when comparing the MAC address of the computers table and the network devices table. If a device is in both lists, Automate determines that the agent is installed and the device is no longer a network device. During the interim period, a device can be in both the network device list and in the agent list.

**Note:** Network probe computers check in every 60 seconds.

## Learning Materials

### Documentation

- Network Probe Defaults
- Overview Screen
- Network Probe Wizard
- Network Devices Screen
  - Network Devices Tab
  - Found Devices Tab
- Network Map Screen
- Extra Data Fields Screen
- Comments Screen
- Probe Commands Screen
- Probe Events Screen
- SNMP Traps Screen
  - SNMP Traps Received Tab
  - SNMP Trap Receivers Tab
- Syslog Filters Screen
  - Syslog Received Tab
  - Syslog Filters Tab
- TFTP Server Screen
- Settings Screen
  - Subnet Tab
  - Scan Tab
  - SNMP Tab
  - Receive Tab
  - Deployment Tab
- Network Devices Screen - Control Center
- Troubleshoot MIB Files
- SNMP Management
- Deleting an Offline Probe

### Blueprints

Do you learn better when you can see the bigger picture? Us too. Check out our blueprints for a birds-eye view of it all. You will be directed to specific key areas of documentation, videos, etc. all within a snazzy infographic.

- Agent Deployment Methods
- Network Probe

### Videos

- How to Make an Agent a Network Probe
- How to Use the Network Probe to Deploy Agents

- How to Use the Network Probe to Discover Assets

### Webinars

We offered a set of live webinars earlier in 2017. In case you missed them, we have added them below for you to reference or watch again!

- Network Probe Part 1 - Introduction
- Network Probe Part 2 - Templates
- Network Probe Part 3 - SNMP Traps

### University Courses

Think you know all there is to know about the Network Probe? Test your knowledge, learn tips and tricks, and earn credit towards a specialized ConnectWise degree by completing the following courses:

- None at this time

## Permissions

The following permissions restrict access to specific actions performed and areas of the Network Probe. If you do not have proper permission you will be notified by the system when attempting to access a specific area or perform a specific function.

**Note:** Permissions that are listed are in addition to basic permissions required to access clients, locations, computers, groups, etc. Refer to Assigning Permissions for additional information on user class permissions, if necessary.

| Task | Class | Level | Category |
|---|---|---|---|
| View network devices (Control Center) and view the individual Network Probe settings | Core | Client | Locations > Read |
| | Core | User | Network Devices > Show all |
| Edit network devices (Control Center) and edit the individual Network Probe settings | Core | Client | Locations > Read<br>Locations > Edit |
| | Core | User | Network Devices > Show all |
| View Network Map (Network Probe tile > Network Map) | Core | Client | Locations > Read |
| | Core | User | Network Devices > Show all |
| Edit the Network Probe default settings (System > Configuration > Network Probe) | Core | User | Network Devices > Show all |