Using NinjaOne to check your managed endpoint devices for Coro Agent

This guide describes how to configure NinjaOne Remote Monitoring and Management (RMM) to check your managed endpoint devices for the presence of the Coro Agent. The automation configured through this process can test endpoint devices and return details of:

- Whether the Coro Agent is installed on a device
- Whether the Coro Agent is running
- Whether the Coro Agent is up-to-date, and the last update time

Prerequisites

Before you begin this guide, make sure you have:

- An active Coro subscription
- Endpoint devices running Coro Agent version 2.5.60.1 (3.1) or later
- Coro's NinjaOne RMM **PowerShell script**
- An active NinjaOne RMM subscription and access to the console
- Your NinjaOne environment is populated with enrolled Windows-based endpoint devices

Setting up an automation in NinjaOne

Coro provides a PowerShell script through which NinjaOne can interrogate endpoint devices for the presence of the Coro Agent. This script references and populates variables matching the names of **Global custom fields** that you must add through the NinjaOne console.

The procedure described in this section covers **adding Global Custom Fields** and then **adding the automation** within which the script resides.

Adding Global Custom Fields

The following table lists fields required by the Coro Agent PowerShell script. For each entry, add a matching **Global Custom Field** using the procedure defined below.