# Integrating Action1 (Remote Monitoring & Management) Into a Help Desk Lab

This walkthrough demonstrates how to install and onboard Windows endpoints into the **Action1** RMM/Endpoint Management platform inside a help desk lab environment.

The goals of this exercise are to practice:

- Creating an Action1 account
- Installing and registering the Action1 agent on Windows machines
- Verifying connectivity and endpoint status
- Running remote commands and remediating vulnerabilities

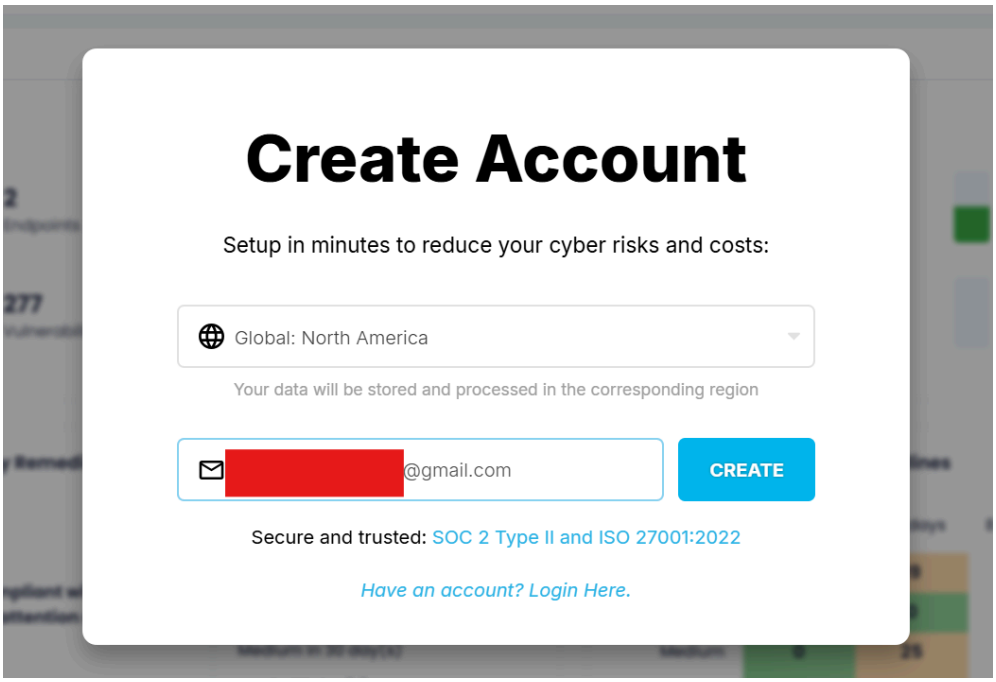
---

# Step 1: Create an Action1 Account

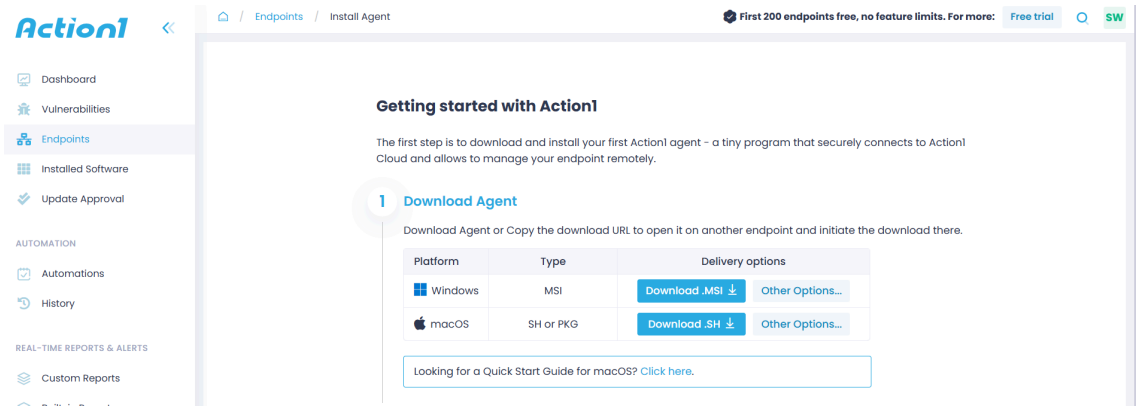
On your Windows 10 VM:

1. Go to the Action1 website.

2. Register for a free account (supports up to 200 endpoints for free).




3. Log in to the Action1 dashboard for the first time.



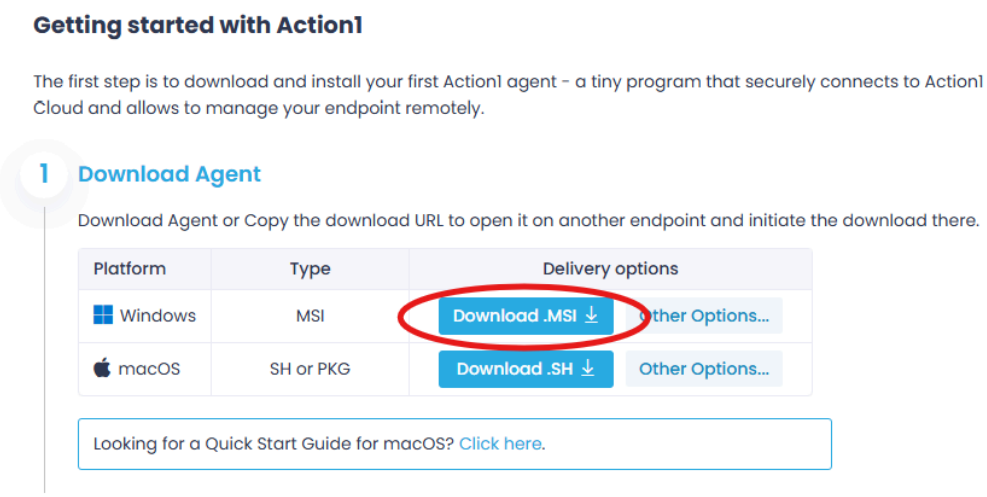
Now you are ready to install the agent on your Windows 10 VM.

---

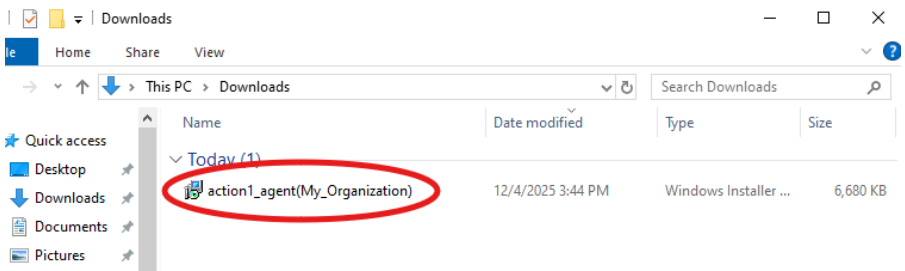
# Step 2: Download the Action1 agent directly inside the VM

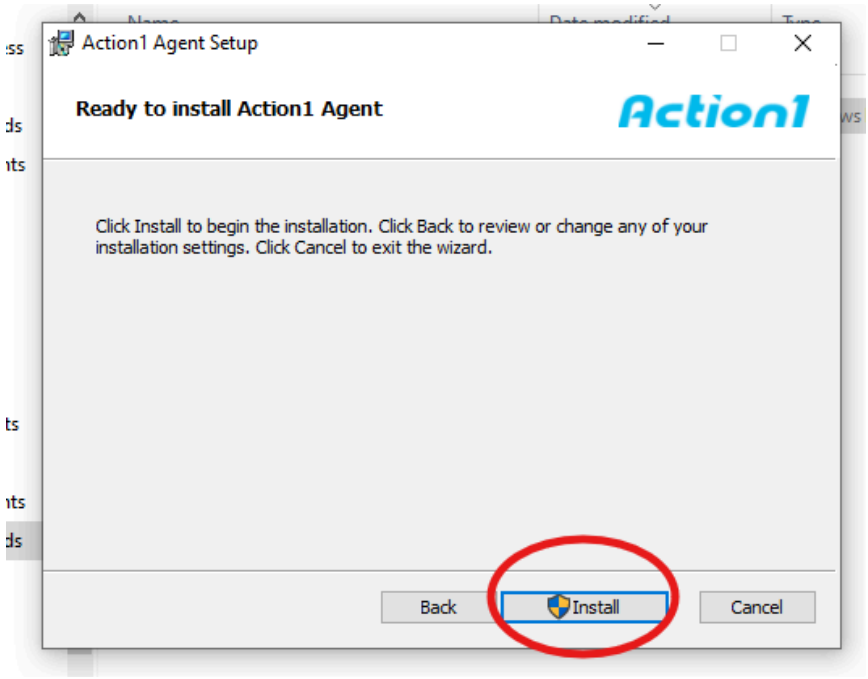
Inside your Windows 10 domain-joined employee workstation:

1. After your first login you will be on the "Getting started with Action1" page. Look at step 1 and download the .msi download agent.



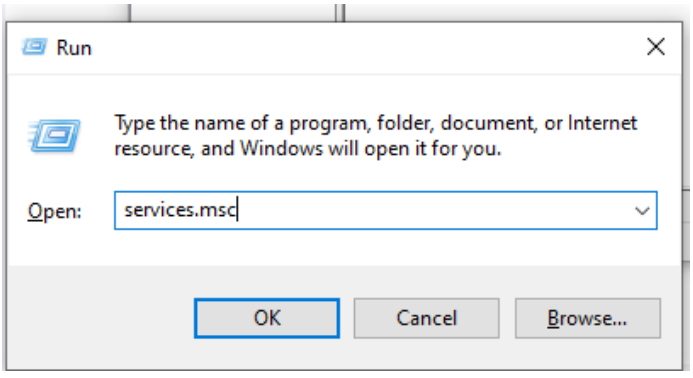

2. Double-click the installer to begin setup. Follow the steps and click **Install**.



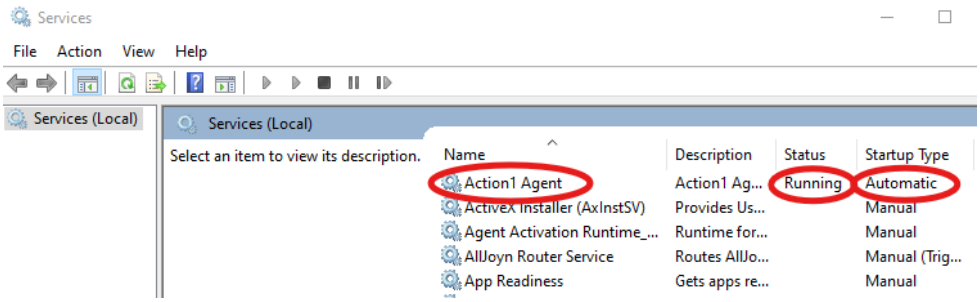



3. Wait for installation to complete (it usually finishes in under 10 seconds).

4. After installation, Press **Windows + R** → type **services.msc** → press **Enter**




5. Locate **Action1 Endpoint Agent** in the list. Status should show **Running.** Startup type should show **Automatic**



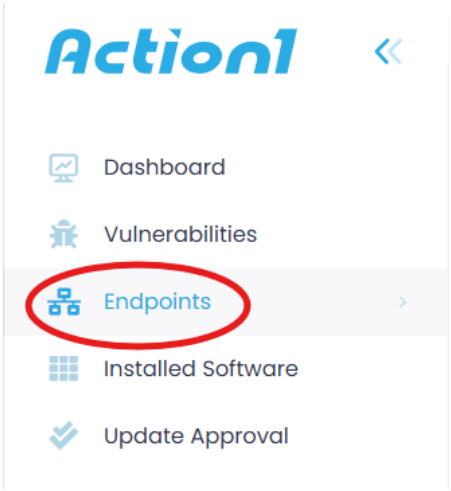

The workstation is now attempting to register with the Action1 cloud.

---

# Step 3: Verify the Endpoint Appears in the Action1 Console

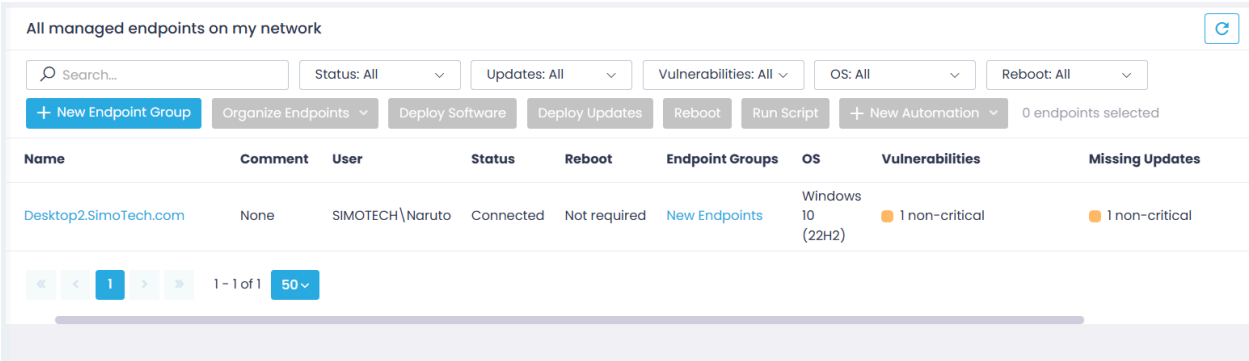
On your host PC inside the Action1 dashboard:

1. Go to the **Endpoints** tab.




You should now see your Windows 10 VM appear with:

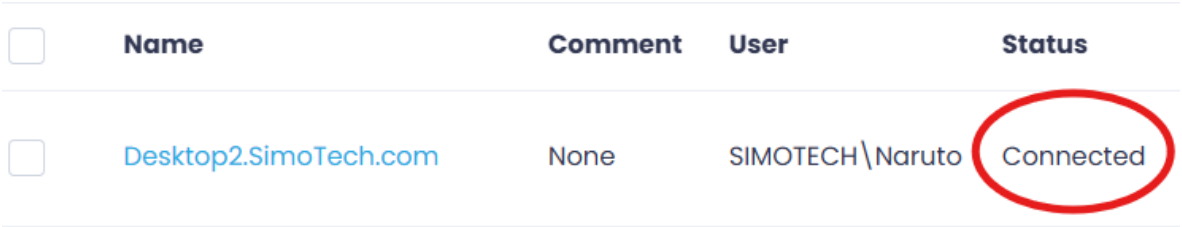
- **Hostname**: Desktop2
- **OS version:** Windows 10
- **Logged-in user:** SIMOTECH\Naruto
- **etc…**




---

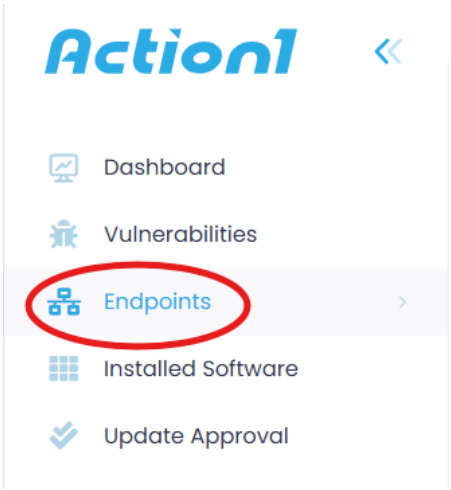
# Step 4: Test Action1 Functionality

Once your endpoint appears and shows **Connected** status, test some of the core features.



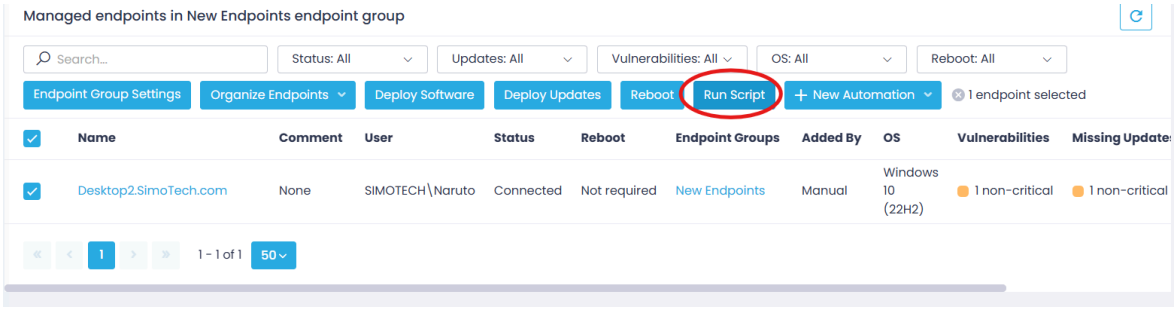

## A. Test Remote Command Execution

1. In Action1, go to **Endpoints**.

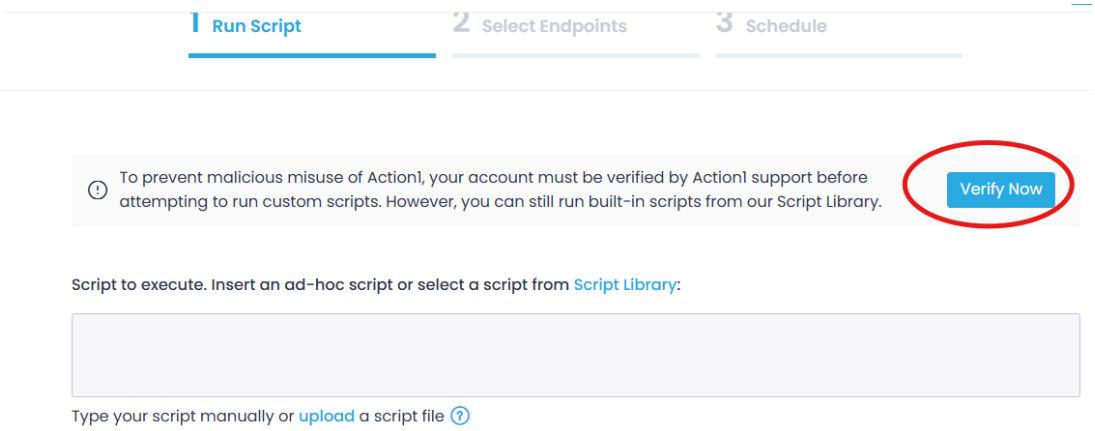


2. Select your Windows 10 workstation.

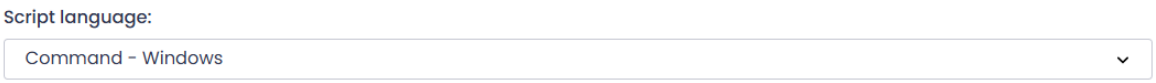
3. Click **Run Script**.



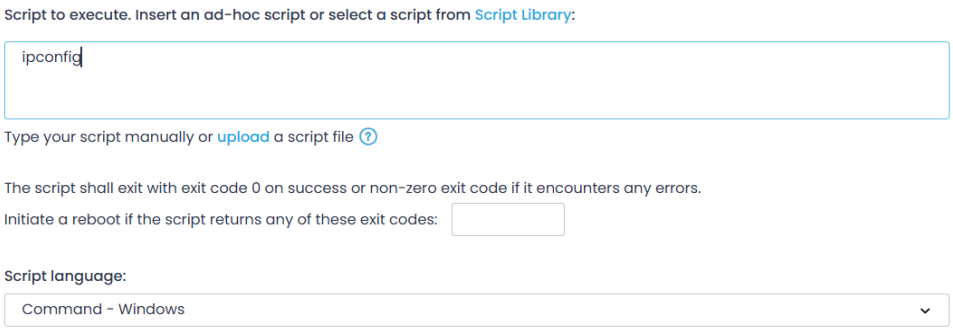

4. In order to run your own scripts you must first click **Verify Now** and follow the verification steps (takes 1 minute).



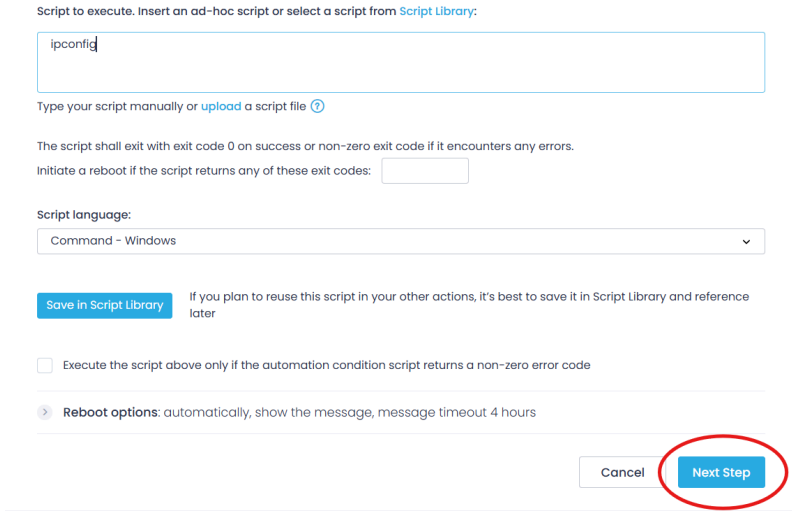

5. Choose **Command Prompt**.



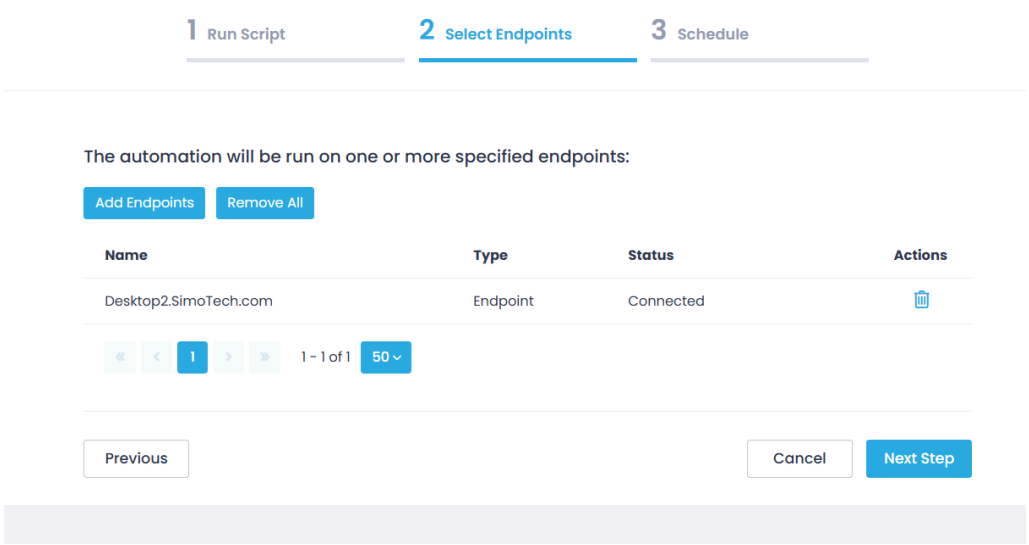

6. Enter: *ipconfig*



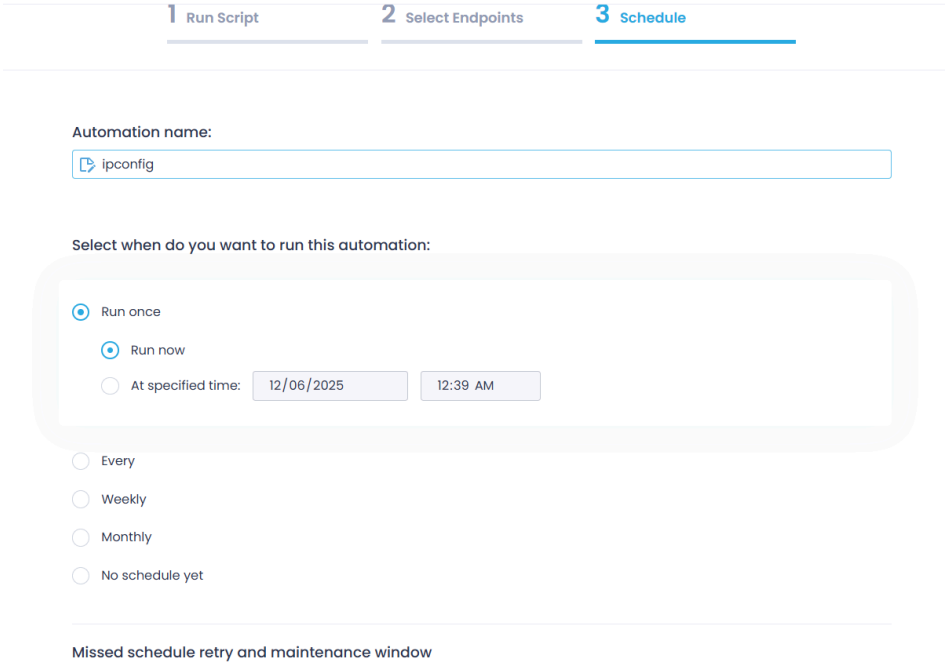

6. Click **Next Step.**



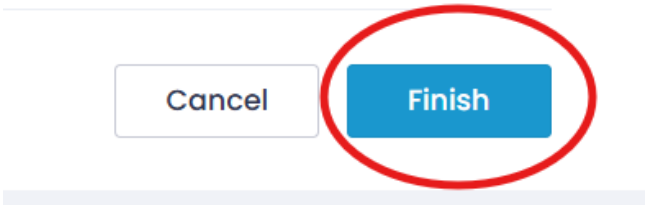

7. Pick the endpoints the script will run on.

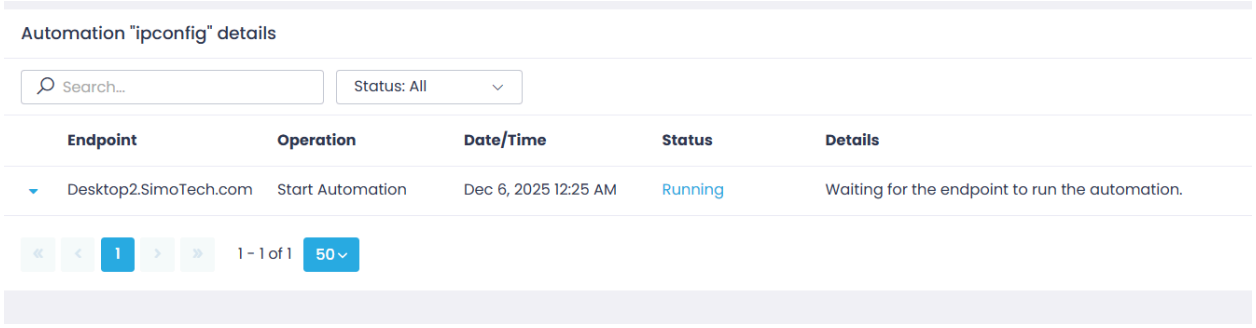


8. Schedule when the script will run. We will schedule it for right now.

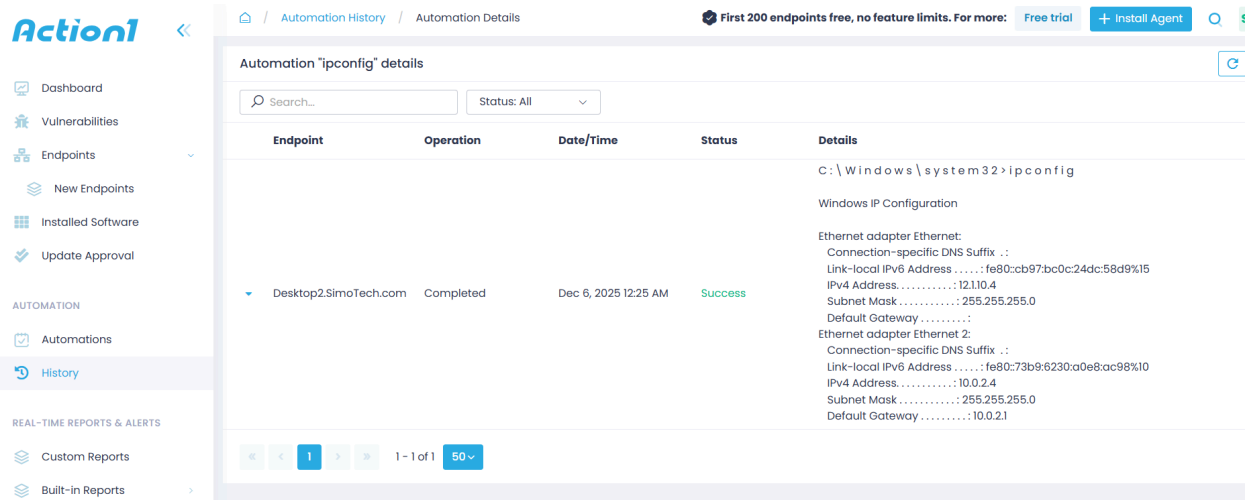



9. Click **Finish**.




10. When the script is done running, the output can be viewed in **Automation History**.

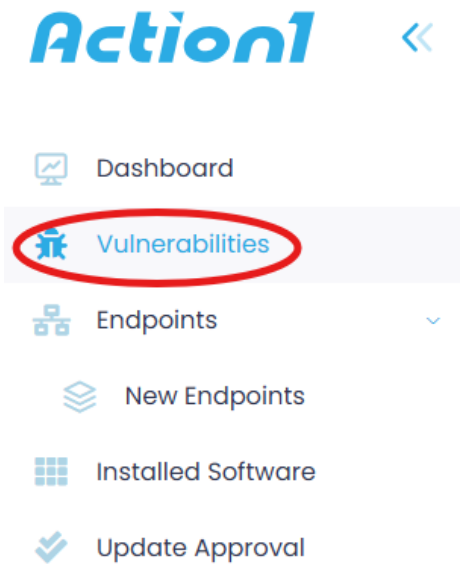



You should see the VM's IP info returned from Action1. Remote command execution is functional.

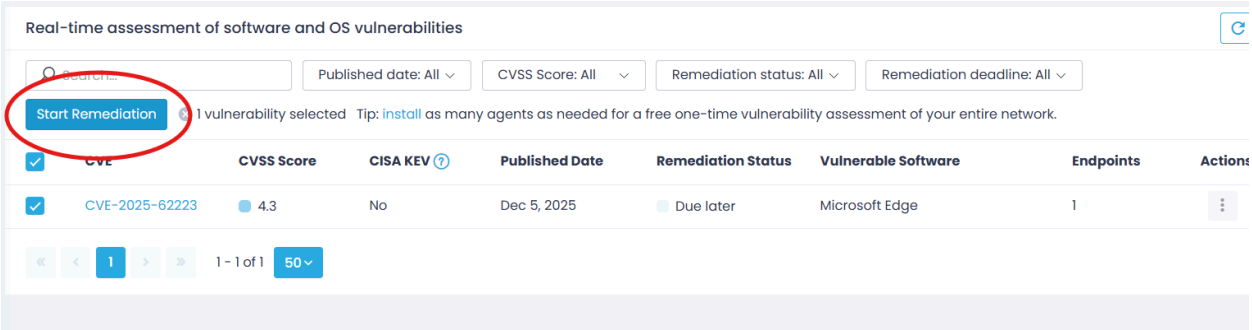
---

## B. Test Vulnerability Remediation

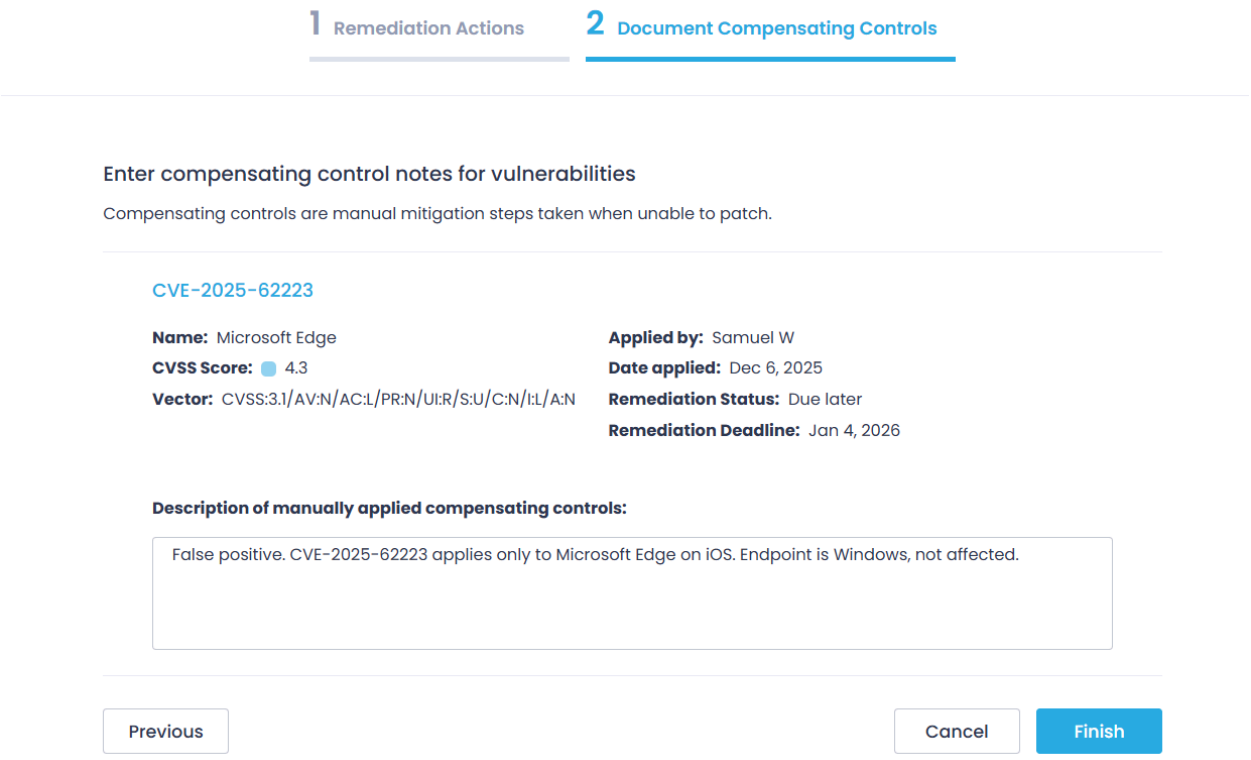
1. Go to **Vulnerabilities**.



2. Click the vulnerability and click **Start Remediation**.




3. This vulnerability, CVE-2025-62223, doesn't actually affect our VM because it only affects Edge on IOS. So we will document this as a false flag.




Vulnerability remediation is confirmed as functional.

## Summary

I integrated the Action1 RMM platform into my help desk lab by creating an account, downloading the Action1 agent directly inside my Windows 10 VM, and confirming that the agent registered correctly in the cloud console. After verifying the service was running, the endpoint appeared in Action1 with full system details.

I tested key features by running a remote command through the “Run Script” tool and reviewing a reported vulnerability, which I documented as a false positive. With Action1 now active in my lab, I can begin performing real-world RMM tasks such as remote troubleshooting, vulnerability review, and automation.

In my next walkthrough, I’ll demonstrate how to remotely deploy software to endpoints using Action1.