

# 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.

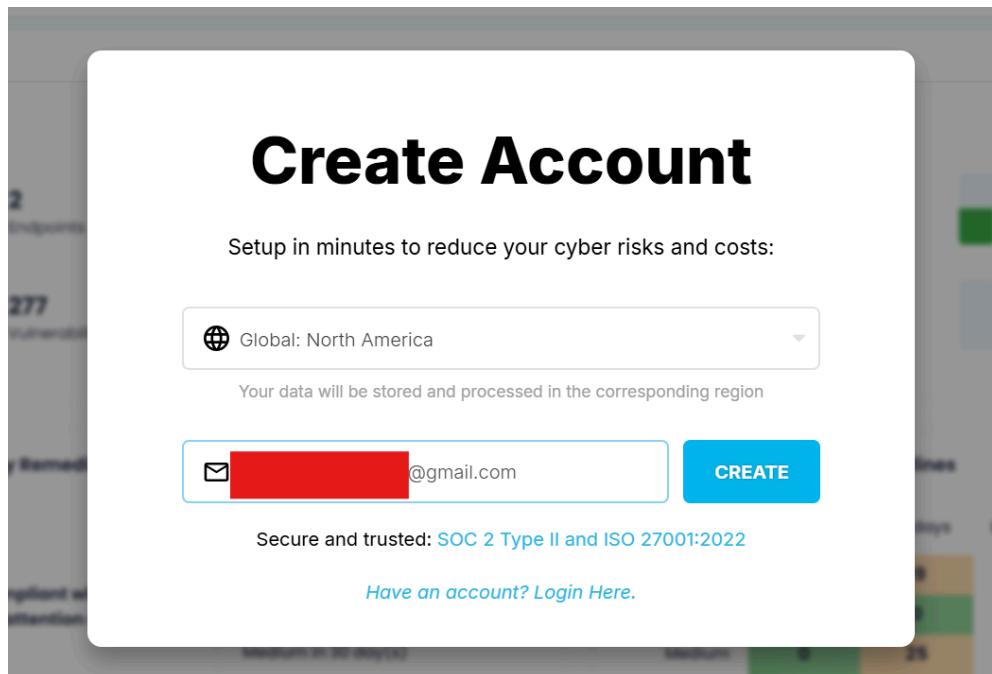
The goals of this exercise are to practice:

- 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.

A screenshot of the Action1 dashboard. The left sidebar has navigation items: Dashboard, Vulnerabilities, Endpoints (which is selected and highlighted in blue), Installed Software, Update Approval, Automations, History, and Real-Time Reports & Alerts. The main content area shows a 'Getting started with Action1' section with a sub-section '1 Download Agent'. It explains the first step is to download and install the agent. Below this is a table for selecting delivery options:

Platform	Type	Delivery options
Windows	MSI	<a href="#">Download .MSI</a> <a href="#">Other Options...</a>
macOS	SH or PKG	<a href="#">Download .SH</a> <a href="#">Other Options...</a>

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.

### Getting started with Action1

The first step is to download and install your first Action1 agent – a tiny program that securely connects to Action1 Cloud and allows to manage your endpoint remotely.

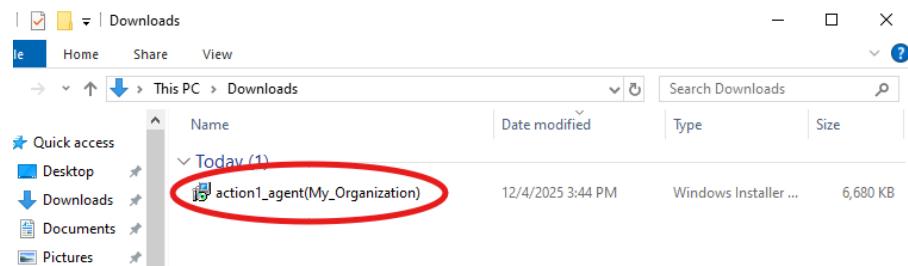
#### 1 Download Agent

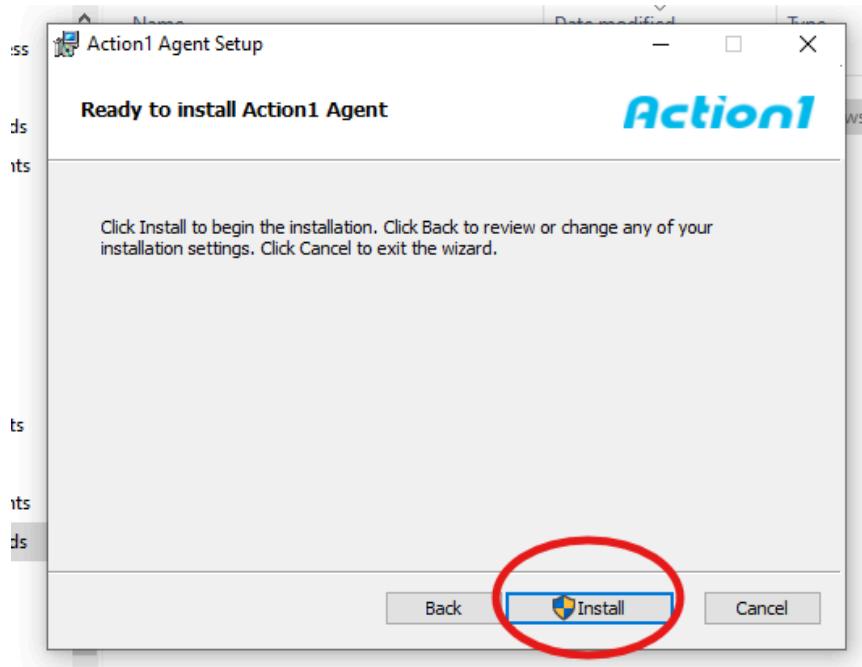
Download Agent or Copy the download URL to open it on another endpoint and initiate the download there.

Platform	Type	Delivery options
Windows	MSI	<a href="#">Download .MSI</a> <a href="#">Other Options...</a>
macOS	SH or PKG	<a href="#">Download .SH</a> <a href="#">Other Options...</a>

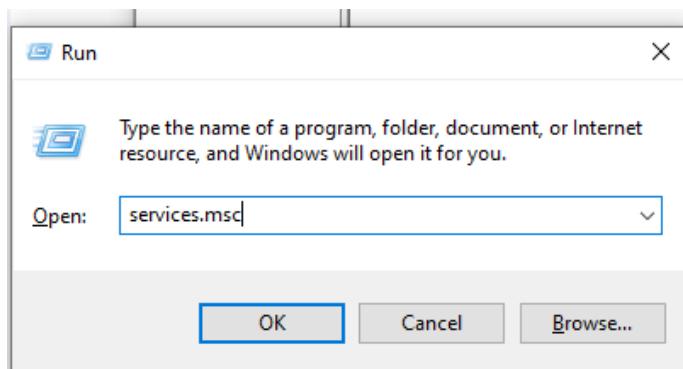
Looking for a Quick Start Guide for macOS? [Click here.](#)

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 screenshot shows the Windows Services console with the title bar "Services". Below it is a toolbar with icons for back, forward, search, and other functions. A left sidebar titled "Services (Local)" contains a message "Select an item to view its description." To the right is a main pane titled "Services (Local)" with a table of services. The table has columns: Name, Description, Status, and Startup Type. The "Action1 Agent" service is highlighted with a red oval. Its details are shown in a tooltip: "Action1 Ag..." (Description), "Running" (Status), and "Automatic" (Startup Type). Other services listed include "Activex Installer (AxInstSV)", "Agent Activation Runtime\_...", "AllJoyn Router Service", and "App Readiness".

Name	Description	Status	Startup Type
Action1 Agent	Action1 Ag...	Running	Automatic
Activex Installer (AxInstSV)	Provides Us...	Manual	Manual
Agent Activation Runtime_...	Runtime for...	Manual	Manual
AllJoyn Router Service	Routes Alljo...	Manual (Trig...	Manual
App Readiness	Gets apps re...	Manual	Manual

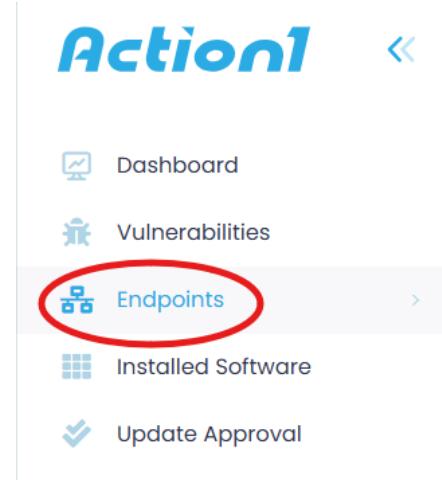
The workstation is now attempting to register with the Action1 cloud.

---

## 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...**

All managed endpoints on my network

Search... Status: All Updates: All Vulnerabilities: All OS: All Reboot: All

+ New Endpoint Group Organize Endpoints Deploy Software Deploy Updates Reboot Run Script + New Automation 0 endpoints selected

Name	Comment	User	Status	Reboot	Endpoint Groups	OS	Vulnerabilities	Missing Updates
Desktop2.SimoTech.com	None	SIMOTECH\Naruto	Connected	Not required	New Endpoints	Windows 10 (22H2)	1 non-critical	1 non-critical

« < 1 > » 1 - 1 of 1 50

## Step 4: Test Action1 Functionality

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

	Name	Comment	User	Status
	Desktop2.SimoTech.com	None	SIMOTECH\Naruto	Connected

### A. Test Remote Command Execution

1. In Action1, go to Endpoints.

Action1

Dashboard

Vulnerabilities

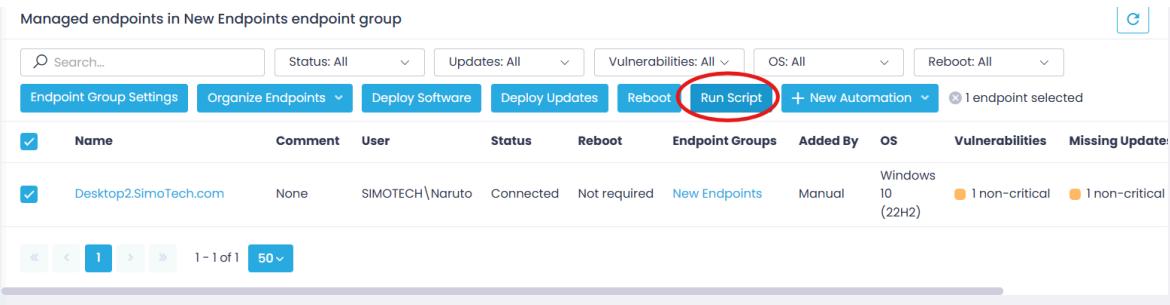
Endpoints

Installed Software

Update Approval

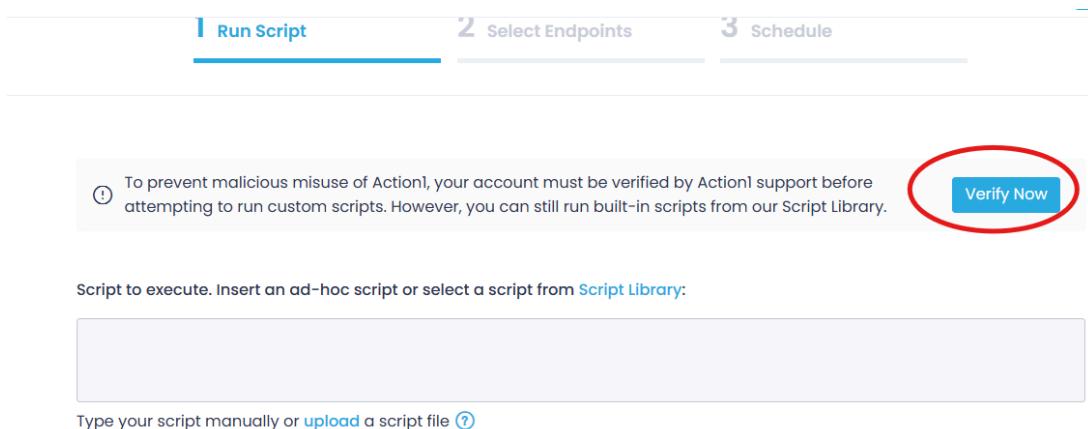
2. Select your Windows 10 workstation.

3. Click **Run Script**.



The screenshot shows a list of managed endpoints. At the top, there are several filter buttons: Search..., Status: All, Updates: All, Vulnerabilities: All, OS: All, and Reboot: All. Below these are buttons for Endpoint Group Settings, Organize Endpoints, Deploy Software, Deploy Updates, Reboot, and Run Script. The Run Script button is circled in red. A '+ New Automation' button and a note indicating '1 endpoint selected' are also present. The main table lists one endpoint: Desktop2.SimoTech.com, which is connected and has no critical vulnerabilities. The interface includes pagination controls at the bottom.

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



The screenshot shows the 'Run Script' step of a process. It includes three tabs: 1 Run Script (highlighted), 2 Select Endpoints, and 3 Schedule. Below the tabs, a note says: 'To prevent malicious misuse of Action1, your account must be verified by Action1 support before attempting to run custom scripts. However, you can still run built-in scripts from our Script Library.' A 'Verify Now' button is circled in red. Below this, there is a text area for inserting a script, with a placeholder 'Script to execute. Insert an ad-hoc script or select a script from Script Library:' and a note: 'Type your script manually or upload a script file'. A small 'Verify Now' button is also visible in the bottom right corner of the main form area.

5. Choose **Command Prompt**.

Script language:

Command - Windows

6. Enter: *ipconfig*

Script to execute. Insert an ad-hoc script or select a script from [Script Library](#):

ipconfig

Type your script manually or [upload](#) a script file (?)

The script shall exit with exit code 0 on success or non-zero exit code if it encounters any errors.

Initiate a reboot if the script returns any of these exit codes:

Script language:

Command - Windows

## 6. Click Next Step.

Script to execute. Insert an ad-hoc script or select a script from [Script Library](#):

ipconfig

Type your script manually or [upload](#) a script file (?)

The script shall exit with exit code 0 on success or non-zero exit code if it encounters any errors.

Initiate a reboot if the script returns any of these exit codes:

Script language:

Command - Windows

[Save in Script Library](#) If you plan to reuse this script in your other actions, it's best to save it in Script Library and reference later

Execute the script above only if the automation condition script returns a non-zero error code

↳ Reboot options: automatically, show the message, message timeout 4 hours

Cancel

Next Step

## 7. Pick the endpoints the script will run on.

1 Run Script

2 Select Endpoints

3 Schedule

The automation will be run on one or more specified endpoints:

[Add Endpoints](#)

[Remove All](#)

Name	Type	Status	Actions
Desktop2.SimoTech.com	Endpoint	Connected	

< < 1 > >> 1 - 1 of 1 50 ▾

[Previous](#)

Cancel

Next Step

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

1 Run Script    2 Select Endpoints    3 Schedule

Automation name:  
ipconfig

Select when do you want to run this automation:

Run once  
 Run now  
 At specified time: 12/06/2025 12:39 AM

Every  
 Weekly  
 Monthly  
 No schedule yet

Missed schedule retry and maintenance window

## 9. Click Finish.

Cancel **Finish**

Automation "ipconfig" details

Search... Status: All

Endpoint	Operation	Date/Time	Status	Details
Desktop2.SimoTech.com	Start Automation	Dec 6, 2025 12:25 AM	Running	Waiting for the endpoint to run the automation.

1 - 1 of 1 50

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

The screenshot shows the Action1 interface. On the left, a sidebar navigation includes: Dashboard, Vulnerabilities, Endpoints (with New Endpoints, Installed Software, and Update Approval), AUTOMATION (with Automations and History), and REAL-TIME REPORTS & ALERTS (with Custom Reports and Built-in Reports). The main content area is titled "Automation 'ipconfig' details". It shows a table with one row for "Desktop2.SimoTech.com" which completed successfully on Dec 6, 2025 at 12:25 AM. The "Details" column displays the output of the ipconfig command, including network adapter information and IP configuration settings.

Endpoint	Operation	Date/Time	Status
Desktop2.SimoTech.com	Completed	Dec 6, 2025 12:25 AM	Success

```
C:\Windows\system32>ipconfig

Windows IP Configuration

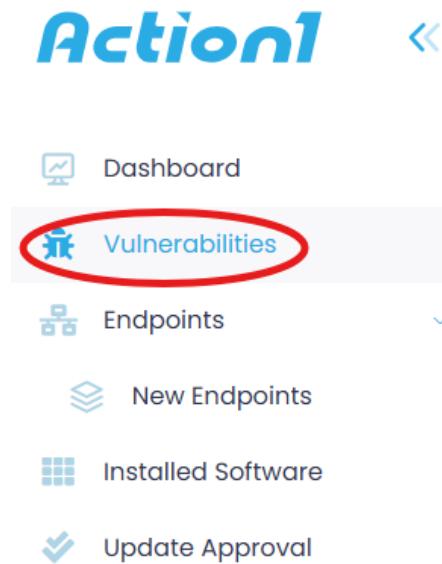
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix .:
  Link-local IPv6 Address . . . . . fe80::cb97:bc0c:24dc:58d9%15
  IPv4 Address . . . . . 12.110.4
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . .
  Ethernet adapter Ethernet 2:
    Connection-specific DNS Suffix .:
    Link-local IPv6 Address . . . . . fe80::73b9:6230:a0e8:ac98%10
    IPv4 Address . . . . . 10.0.2.4
    Subnet Mask . . . . . 255.255.255.0
    Default Gateway . . . . . 10.0.2.1
```

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**.

Real-time assessment of software and OS vulnerabilities

Start Remediation 1 vulnerability selected Tip: [Install](#) as many agents as needed for a free one-time vulnerability assessment of your entire network.

CVE	CVSS Score	CISA KEV	Published Date	Remediation Status	Vulnerable Software	Endpoints	Actions
CVE-2025-62223	4.3	No	Dec 5, 2025	Due later	Microsoft Edge	1	

1 - 1 of 1 50

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.

**1 Remediation Actions**

**2 Document Compensating Controls**

---

Enter compensating control notes for vulnerabilities

Compensating controls are manual mitigation steps taken when unable to patch.

---

**CVE-2025-62223**

**Name:** Microsoft Edge      **Applied by:** Samuel W

**CVSS Score:** 4.3      **Date applied:** Dec 6, 2025

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N      **Remediation Status:** Due later

**Remediation Deadline:** Jan 4, 2026

**Description of manually applied compensating controls:**

False positive. CVE-2025-62223 applies only to Microsoft Edge on iOS. Endpoint is Windows, not affected.

---

[Previous](#) [Cancel](#) [Finish](#)

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.