

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.

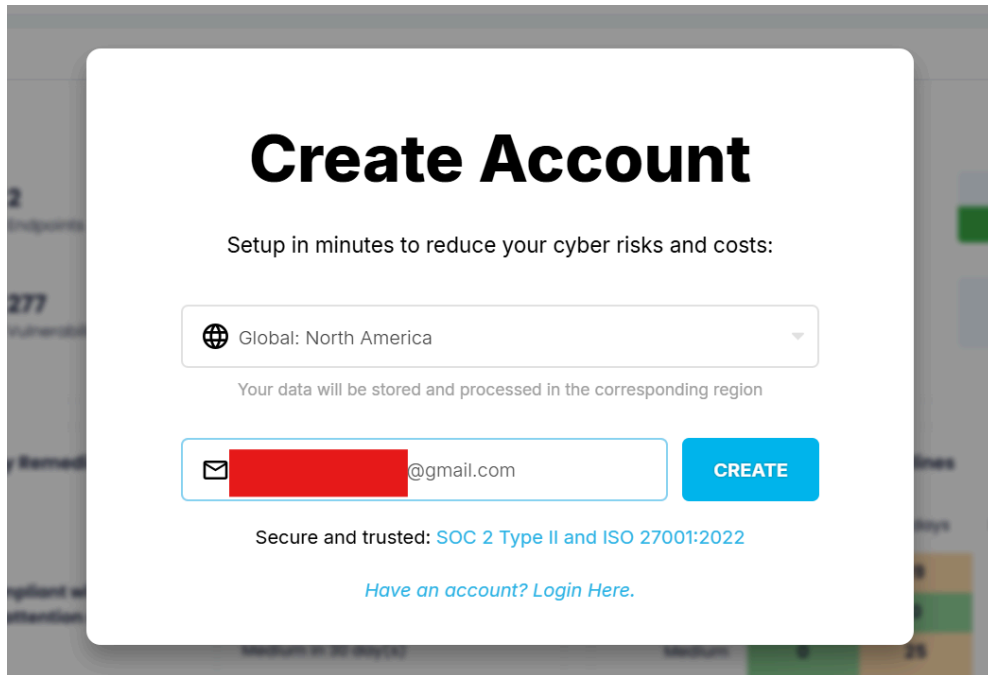
The goals of this exercise are to practice:

- 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).



The screenshot shows a 'Create Account' modal window. At the top, it says 'Create Account' in large bold letters, followed by 'Setup in minutes to reduce your cyber risks and costs:'. Below this is a dropdown menu for region selection, currently showing 'Global: North America'. A note states 'Your data will be stored and processed in the corresponding region'. There is an email input field with a redacted address and a blue 'CREATE' button. At the bottom, it mentions 'Secure and trusted: SOC 2 Type II and ISO 27001:2022' and provides a link 'Have an account? Login Here.'

Create Account

Setup in minutes to reduce your cyber risks and costs:

Global: North America ▼

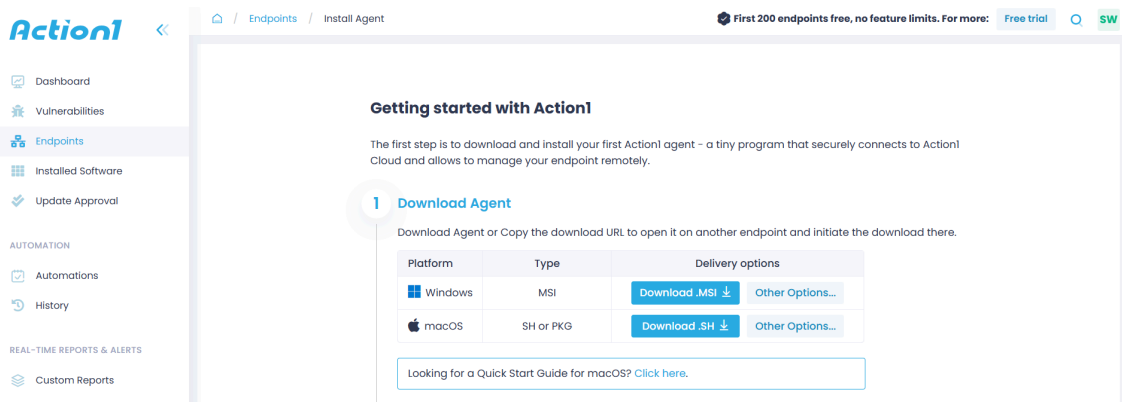
Your data will be stored and processed in the corresponding region

✉ [Redacted]@gmail.com **CREATE**

Secure and trusted: [SOC 2 Type II and ISO 27001:2022](#)

[Have an account? Login Here.](#)

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



The screenshot shows the Action1 dashboard. The left sidebar contains navigation links: Dashboard, Vulnerabilities, Endpoints (selected), Installed Software, Update Approval, AUTOMATION, Automations, History, REAL-TIME REPORTS & ALERTS, Custom Reports. The main content area is titled 'Getting started with Action1' and includes a sub-header '1 Download Agent'. It explains that the first step is to download and install the Action1 agent. Below this is a table with download options for Windows and macOS.

Action1 << / Endpoints / Install Agent

First 200 endpoints free, no feature limits. For more: [Free trial](#) [SW](#)

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	Download .MSI ↓	Other Options...
macOS	SH or PKG	Download .SH ↓	Other Options...

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

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.

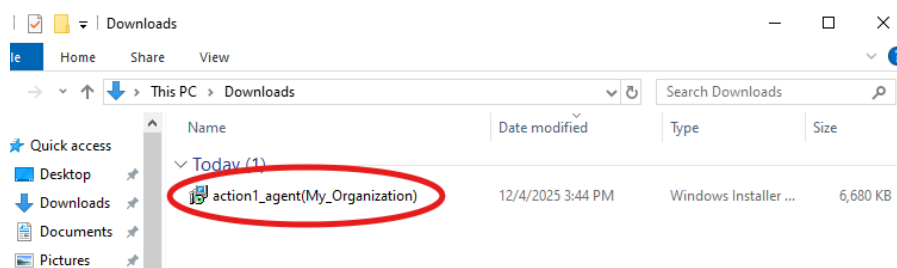
1 Download Agent

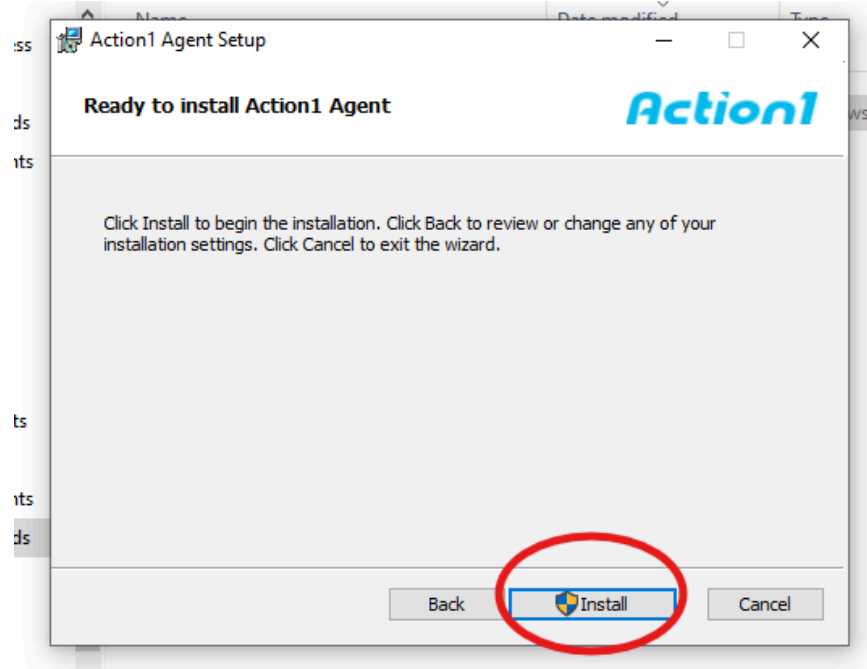
Download Agent or Copy the download URL to open it on another endpoint and initiate the download there.

Platform	Type	Delivery options	
 Windows	MSI	Download .MSI ↓	Other Options...
 macOS	SH or PKG	Download .SH ↓	Other Options...

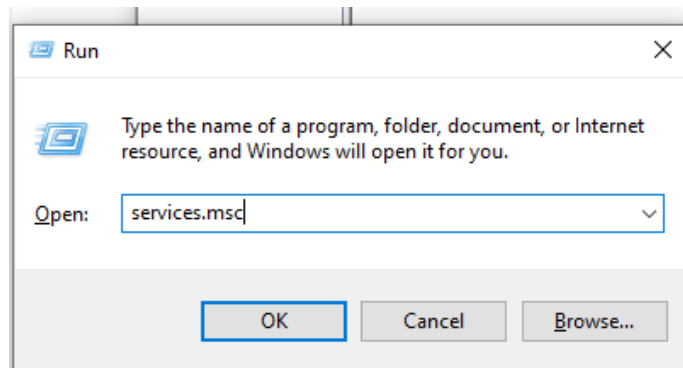
Looking for a Quick Start Guide for macOS? [Click here.](#)

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

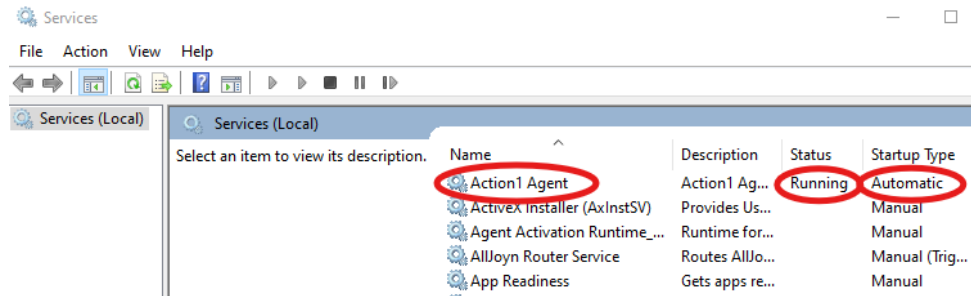




3. Wait for installation to complete (it usually finishes in under 10 seconds).
4. After installation, Press **Windows + R** → type **services.msc** → press **Enter**



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

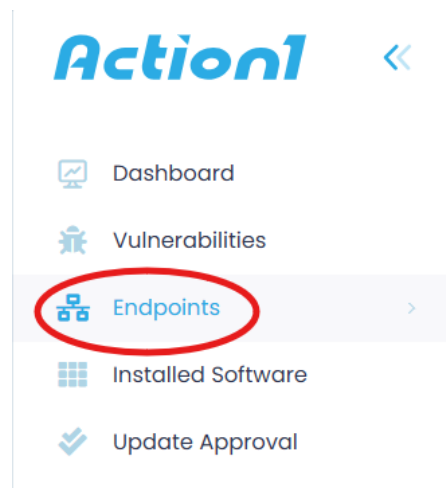


The workstation is now attempting to register with the Action1 cloud.

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 🔄

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

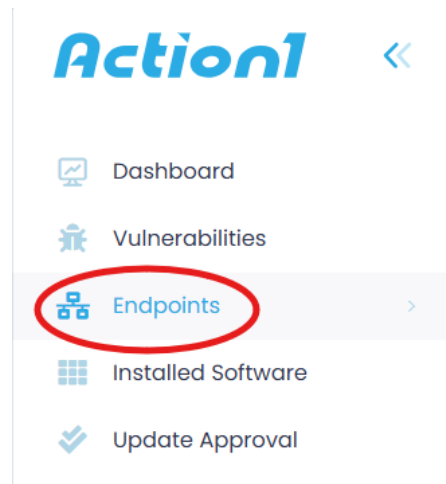
Step 4: Test Action1 Functionality

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

<input type="checkbox"/>	Name	Comment	User	Status
<input type="checkbox"/>	Desktop2.SimoTech.com	None	SIMOTECH\Naruto	Connected

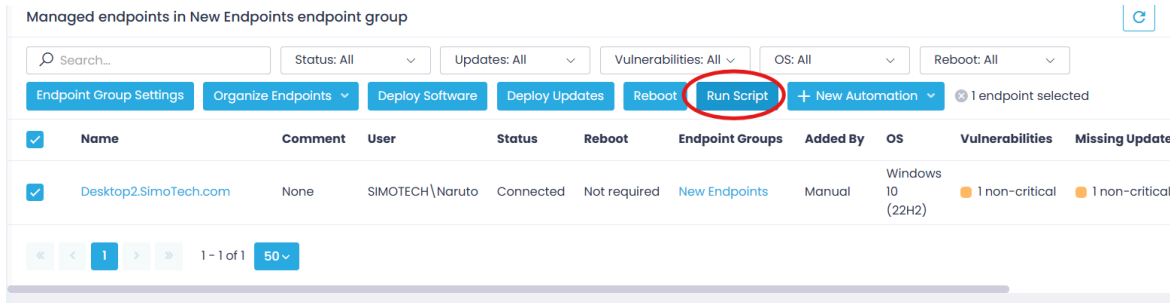
A. Test Remote Command Execution

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

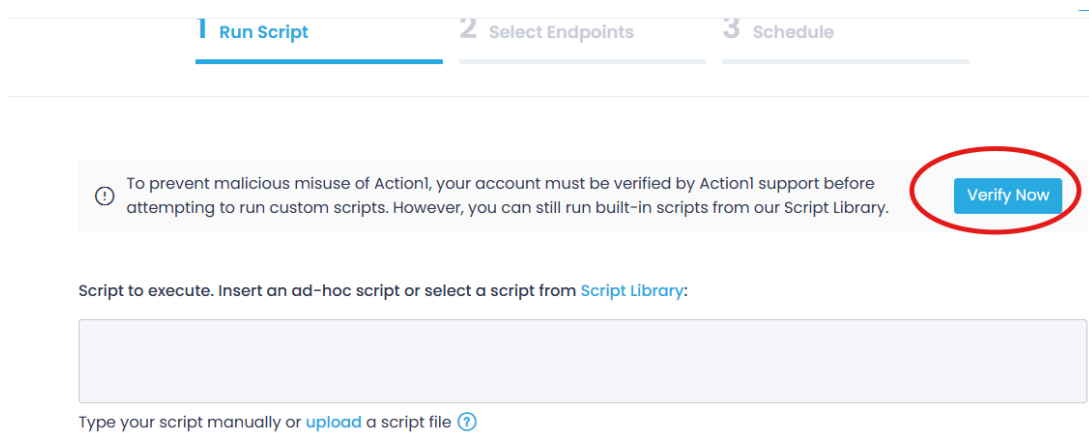


2. Select your Windows 10 workstation.

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*

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				
<input type="text" value="Search..."/>		Status: All <input type="button" value="v"/>		
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.
<div><div><div><<</div><div><</div><div>1</div><div>></div><div>>></div></div><div>1 - 1 of 1</div><div>50 <input type="button" value="v"/></div></div>				

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

The screenshot shows the Action1 interface with the 'Automation History' page selected. The left sidebar contains navigation options: Dashboard, Vulnerabilities, Endpoints, New Endpoints, Installed Software, Update Approval, AUTOMATION, Automations, History (selected), REAL-TIME REPORTS & ALERTS, Custom Reports, and Built-in Reports. The main content area displays 'Automation "ipconfig" details'. At the top, it says 'First 200 endpoints free, no feature limits. For more: Free trial + Install Agent'. Below this is a search bar and a 'Status: All' dropdown. The main table has columns: Endpoint, Operation, Date/Time, Status, and Details. One entry is visible for 'Desktop2.SimoTech.com' with a 'Completed' status on 'Dec 6, 2025 12:25 AM'. The 'Details' column shows the output of the 'ipconfig' command, including network configuration for two Ethernet adapters. At the bottom, there is a pagination bar showing '1 - 1 of 1' and a '50' dropdown.

Endpoint	Operation	Date/Time	Status	Details
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**.

The screenshot shows the Action1 dashboard. The left sidebar contains navigation options: Dashboard, Vulnerabilities (highlighted with a red circle), Endpoints, New Endpoints, Installed Software, and Update Approval. The main content area is currently empty.

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

Real-time assessment of software and OS vulnerabilities

Search: Published date: All CVSS Score: All Remediation status: All Remediation deadline: All

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

<input checked="" type="checkbox"/>	CVE	CVSS Score	CISA KEV	Published Date	Remediation Status	Vulnerable Software	Endpoints	Actions
<input checked="" type="checkbox"/>	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.