

[HOME](#) / [SUPPORT](#) / [AGENTS](#) / [INSTALLING AUTHENTICATION VERIFIER AGENTS](#)

# Support

## Support Categories

### AUTHENTICATION VERIFIER AGENTS

# Installing Authentication Verifier Agents

#### THIS DOCUMENT IS FOR:

Invicti Enterprise On-Demand, Invicti Enterprise On-Premises

Feedback



You can download and install authentication verifier agents to verify that you run authenticated scans in your local environment.

To help secure all parts of your web applications, you can download and install authentication verifier agents.

- In order to scan a website located on your internal network, and not accessible from the internet, you can install and configure a **scan agent** on your network. The agent will conduct the actual scan job and then report the results back to Invicti Enterprise.
- You can download and install an internal verifier agent to perform the authentication, so you can make sure that your scan is authenticated.

For further information about the internal authentication verifier, see [Streamline authenticated scanning with Invicti's verifier agents](#).

This topic explains how to install, update, and uninstall authentication verifier agents on Windows. Using Linux? See [Installing Authentication Verifier Agent on Linux \(Debian Distribution\)](#). For the RedHat distributions, see [Installing Authentication Verifier Agent on Linux \(RedHat Distribution\)](#).

The Authentication Verifier Agent is an **optional** component.

Download and install the authentication verifier agent if you need to scan websites with form or basic authentication or OAuth2. The authentication verifier agents also work for the Authentication Profiles, Custom Scripts for Form Authentication, CyberArk Vault, HashiCorp Vault, and AzureKey Vault.

## Downloading and configuring authentication verifier agent

There are 3 steps in this process:

- . Downloading an authentication verifier agent
- . Configuring an authentication verifier agent
- . Setting an authentication verifier agent as a Windows Service

## Prerequisites

### Software Requirements

- Windows Server 2016 or above (Windows Server 2019 recommended)

### Hardware Requirements

- 1.4 GHz Processor (2.0 GHz or faster recommended)
- 4 GB RAM or higher recommended
- 10 GB Free Disk space for each internal agent

If you select TLS 1.3 as a security protocol from the [Scan Policy](#), make sure you have Windows 11 or Windows Server 2022 or higher versions.

## Network Requirements

- Agent should be configured so that it can reach your internal website through HTTP/HTTPS
- Agent needs to be able to access the Invicti Enterprise Application Server's HTTP(S) (443) port

## Allowlisting Requirements

- www.invicti.com
- r87.me
- Allowlist the following addresses according to your region:
  - US region: 34.237.50.127, us-avservice.netsparkercloud.com, s3.us-east-1.amazonaws.com
  - EU region: 18.193.27.197, eu-avservice.netsparker.cloud, s3.eu-central-1.amazonaws.com
  - CA region: 52.60.130.46, ca-avservice.netsparker.cloud, s3.ca-central-1.amazonaws.com

Feedback

## Required Access

- User(s) must have administrator privileges to run the required commands and agent service.

## Step 1. Downloading the authentication verifier agent

You need to download the authentication verifier agent and install it on a machine in your internal network.

## How to download the authentication verifier agent

- Log in to Invicti Enterprise.
- From the main menu, go to **Agents > Manage Agents > Configure New Agent**.
- From the **Authentication Verifier** section, select **Windows** to download the file.

**Configure New Agent**

Download Invicti Enterprise Scanner Agent and you can start using it with this Agent Token. [See the installation document.](#)

**Agent (v23.3.0)**

Please select the platform below.

Windows Linux Docker OpenShift

**Authentication Verifier (v23.3.0)**

Please select the platform below.

Windows Linux

**Agent Token** ⓘ

N/9 siDmrU=

**Reset Agent Token**

**Available Agents**

No agents detected. You need to install, at least, one agent in order to launch internal scans.

Feedback

When you download the zip file, you can configure the authentication verifier agent.

## Step 2. Configuring authentication verifier agent

### How to configure the authentication verifier agent

- Navigate to the folder you downloaded the zip file.
- Extract the contents of the zip file to C:\NC\_VerifierAgent. (You can use another location, but this instruction will use this path.)

- . Open the C:\NC\_VerifierAgent\appsettings.json file with your preferred text editor.
- . Edit the following attributes before running the agent, listed under AgentInfo:
  - **AgentName:** This can be anything you want. (If you are going to install more than one instance of the agent, you must set a unique agentName value for each instance, something you will use later.)
  - **ApiToken:** In Invicti Enterprise, the Agent Token is displayed in the Configure New Agent window. Copy the value into the apiToken.

Do not edit the ApiRootUrl address. If edited, your authentication verifier agent may not work.

Allowlist the ApiRootUrl address so that the authentication verifier agents can access the verifier server for the form authentication.

Make sure the machine where the authentication verifier agent is installed can access the ApiRootURL.

Feedback

- . Save and close the C:\NC\_VerifierAgent\appsettings.json file.

### Changing default data folder for the authentication verifier agent

You can change the default location in which the scanner agent saves its data. For further information, refer to Changing default data folder for the authentication verifier agent.

## Setting proxy in authentication verifier agent

You can set a proxy for the authentication verifier agent in Invicti Enterprise. Invicti supports Basic Authentication but not Digest and NTLM.

You are required to manually enter proxy settings into the appsettings.json file with your preferred text editor.

This table lists and explains the entries in the Proxy settings.

Field	Description
Proxy Mode	<p>Enter your proxy settings if you want the Agent to use or not to use the proxy. There are three modes:</p> <p><b>NoProxy:</b> The Agent does not use a proxy even if you configure the server's proxy settings.</p> <p><b>SystemProxy:</b> The Agent uses the System Proxy that was defined on the server.</p> <p><b>CustomProxy:</b> The Agent uses Custom Proxy that you define in the appsettings.json file.</p>
Use Default Credentials	Enter true if you authenticate to the proxy via the user that the Agent service is defined.
Username	Enter a username for authentication
Password	Enter a password for authentication
Domain	Enter a domain name
Address	Enter a proxy address. Only IP address or hostname without schema and port is allowed.
Port	Enter a port for the proxy
Bypass on Local	Enter a value that indicates whether to bypass the proxy server for local addresses.
Bypass List	<p>Enter the address(es) that do not use the proxy server. Enter the address(es) as RegEx.</p> <p>The following shows some possible bypass list expressions:</p> <p>"example\\.com",</p> <p>";*\\.example\\.com",</p> <p>"192\\.168\\.1\\.1",</p> <p>"www\\.example\\.com",</p> <p>"www\\.example\\.com:8080",</p> <p>"100\\.;*\\.;*\\.*"</p>

Feedback

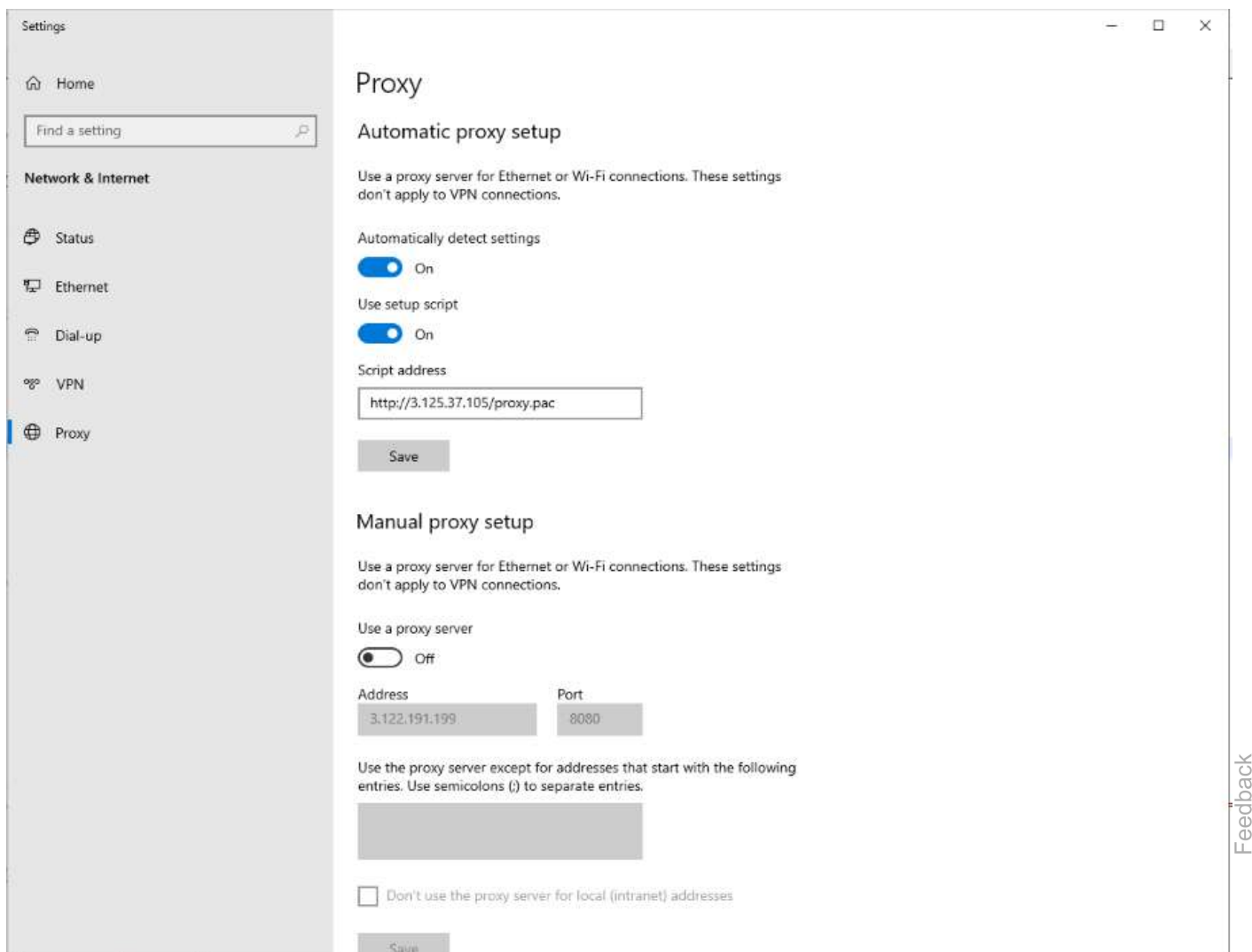
## Using Proxy Auto-Configuration file

You can use Proxy Automatic Configuration (PAC) to configure your proxy. A PAC file lets you describe the proxy configuration in a file using JavaScript, so you can manage your proxy settings.

To use a PAC file, you must set the Proxy Mode to System Proxy in the appsetting.json file.

### *How to use a Proxy Auto-Configuration file on Windows*

- . Go to **Settings > Network & Internet > Proxy**.
- . Turn on the Use setup script toggle.
- . In the Script address field, enter the PAC file's URL address.



- . Select **Save**.

## Step 3. Setting authentication verifier agent as a Windows Service

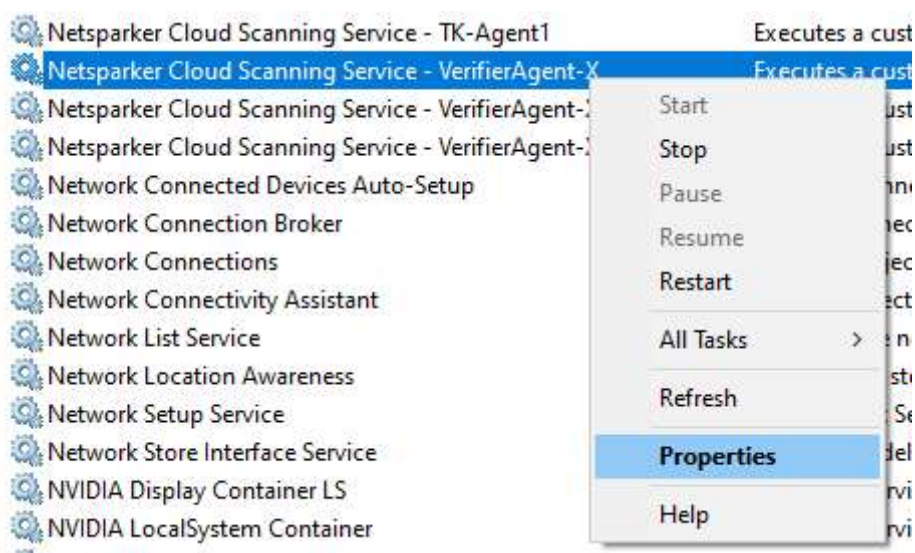
An internal authentication verifier agent should be configured as a Windows service so that it can poll the Invicti Enterprise servers regularly and can take the verification initiation command from the server.

### *How to set the authentication verifier agent as a Windows Service*

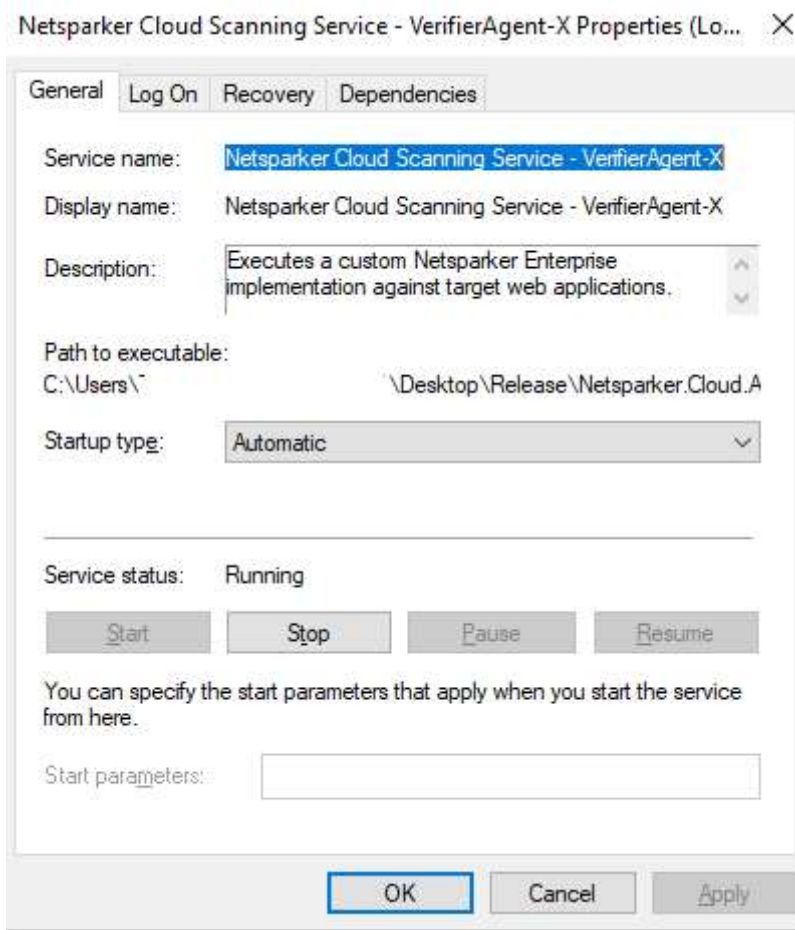
- . Open a command prompt in Administrator mode and navigate to the agent's folder.



- Run the following command to install the Invicti Enterprise Authentication Verifier Agent as a Windows Service: `Netsparker.Cloud.Agent.exe -i`
- Press **Windows+R**, type 'services.msc' and press **Enter**.
- Find 'Invicti Enterprise Scanning Service – [YOUR\_AGENT\_NAME]'.



- Right-click on it and select **Properties**.
- Make sure Startup type is set to Automatic, and select **Start**.



Feedback

- Select **Apply** and **OK**, then exit the Properties window.

Although this service is set to start automatically, it may not restart until the PC is restarted too.

After these steps, the Invicti Enterprise Authentication Verifier Agent should be running on your network. To view your verifier agents, from the main menu, select **Agents > Manage Verifiers**.

Manage Auth Verifiers						
Name	Last Verification Date	Last Heartbeat	Agent Version	Auto Update Enabled	Vdb Version	Operating System
AV-Agent1	12/16/2022 2:16 AM	2.0.2.151	Yes	202207291500	Microsoft Windows 10.0.19044	<div>✖ Delete</div> <div>⚡ Commands ▾</div>

Any change in the appsetting.json file, such as setting proxy and changing API Token, requires restarting the service so that the changes can take effect.

## Updating authentication verifier agents

There are three methods to update your authentication verifier agent.



- When a new verifier agent version has been published, you can update your Agents manually using installation files on the machines on which agents are installed.
- You can update agents manually by selecting Update Agent (visible only when the Enable Auto Update is not configured and the new version of the Agent is available). While the update is in progress, the State field will display 'Updating'.
- You can enable the auto update feature. The target verifier agent updates itself as soon as possible when it's idle.

Feedback

### *How to enable automatic Authentication Verifier Agent updates*

- From the main menu, select **Agents > Manage Verifiers**.
- Next to the relevant agent, select the **Command** drop-down, then **Enable Auto Update**.

Manage Auth Verifiers						
Name	Last Verification Date	Last Heartbeat	Agent Version	Auto Update Enabled	Vdb Version	Operating System
AV-Agent1		12/16/2022 2:16 AM	2.0.2.151	Yes	202207291500	Microsoft Windows 10.0.19044

 Delete  Commands

## Changing default data folder for the authentication verifier agent

You can change the default location where the authentication verifier agent saves its data. This helps you avoid running out of free space due to accumulating data.

By default, the authentication verifier agent saves the data to the C:/Invicti Enterprise folder. But, you can choose to save the data in a different location to prevent filling up your free space.

The following instruction explains how to change the location where the authentication verifier agent saves its data. The instruction is valid for new agents or existing agents:

### *How to change the default data folder*

- . Navigate to the agent's folder you want to change the default folder.
- . Open appsettings.json file with your preferred text editor.
- . Add the following attribute listed under AgentInfo: **"ScanDataFolderPath":**  
**"FullPath"**

Write the full path as shown in the following example: C:\\Users\\  
[User]\\Documents\\ScanData

Feedback

- . Save and exit.

If you modified the existing agent's configuration file, you need to restart the agent service. So, Open services.msc, find 'Netsparker Cloud Scanning Service – [YOUR\_AGENT\_NAME]', and restart the agent service.

This restart does not affect your saved data. To move the existing data, you need to copy the data and paste it into the new folder.

If this is a new agent, continue following this instruction: [Step 2. Configuring authentication verifier agent](#)

## **Installing multiple authentication verifier agents on Windows**

- Copy all files from the default Verifier Agent's folder to the new Agent's folder. The path is: **C:\Invicti Enterprise Agent**.

For example, if you decided to use **Agent-2** as the new Agent name, you could use this command to copy all files to new Agent's folder:

```
xcopy "C:\Invicti Enterprise Agent\*.*" "C:\Invicti Enterprise Agent-2" /yie
```

This creates a new directory in **C:\Invicti Enterprise Agent-2** and copies in all the required files.

- Locate the new Agent's folder and open the **appsettings.json** file with a text editor. Set the new Agent's name.
- Open a command prompt in Windows with *Administrator* rights and install the new Agent as a Windows Service using these commands:
  - This command changes the current folder to the new Agent's folder: `cd C:\Invicti Enterprise Agent-2`
  - This command installs the new Agent as a Windows Service:  
`Netsparker.Cloud.Agent.exe -i`

Feedback

## Uninstalling the authentication verifier agent

You can uninstall verifier agents.

### *How to uninstall the authentication verifier agent*

- Open a command prompt in Administrator mode and navigate to the agent's folder.
- Run the following command to stop and delete the Invicti Enterprise Authentication Verifier Agent as a Windows Service:
  - `sc stop "Invicti Cloud Scanning Service - YourAgentName"`
  - `sc delete "Invicti Cloud Scanning Service - YourAgentName"`

These commands stop and delete the verifier agent service. If required, you can delete the related folder.

Tweet

Share

Share

Email

TOP ARTICLES

- What is Invicti?
- Overview of Scan Policies
- Scheduling Scans
- Managing Integrations
- Built-In Reports

Feedback

Invicti Help Center

Our Support team is ready to provide you with technical help.

Go to Help Center ►

This will redirect you to the ticketing system.



Invicti Security Corp 1000 N Lamar Blvd Suite 300 Austin, TX 78703, US

## RESOURCES

Features  
Integrations  
Plans  
Case Studies  
Advisories  
Invicti Learn

## USE CASES

Penetration Testing Software  
Website Security Scanner  
Ethical Hacking Software  
Web Vulnerability Scanner  
Comparisons  
Online Application Scanner

## WEB SECURITY

The Problem with False Positives  
Why Pay for Web Scanners  
SQL Injection Cheat Sheet  
Getting Started with Web Security  
Vulnerability Index  
Using Content Security Policy to Secure Web Applications

## COMPANY

About Us  
Contact Us  
Support  
Careers  
Resources  
Partners

© Invicti 2023

## Legal

Privacy Policy  
California Privacy Rights  
Terms of Use

**Accessibility**  
**Sitemap**

Feedback