

Prerequisites:

To get the Nginx Renewal Agent working smoothly with your deployed instance of CertSecure Manager, you'll need a few key things.

1. Administrative privileges

You must be logged in as a local administrator on the target machine where you want to install the agent and the Nginx webserver is running.

2. Connectivity:

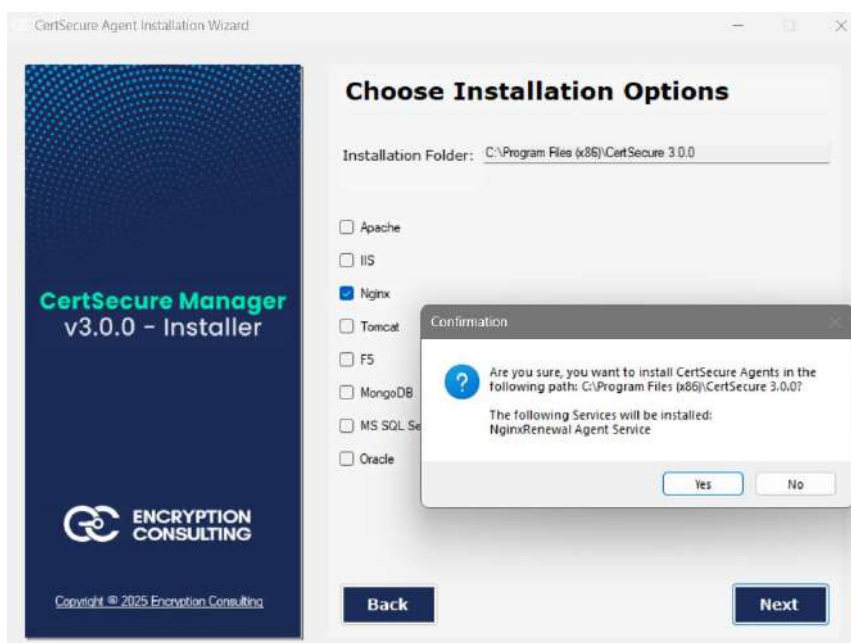
CertSecure Manager must be accessible from the machine running the webserver. To validate, try visiting <https://your-certsecure-backend-url/check> using a browser.

Installation

After confirming the prerequisites, you can set up the renewal agent using the installer.

1. Configuration and Installation

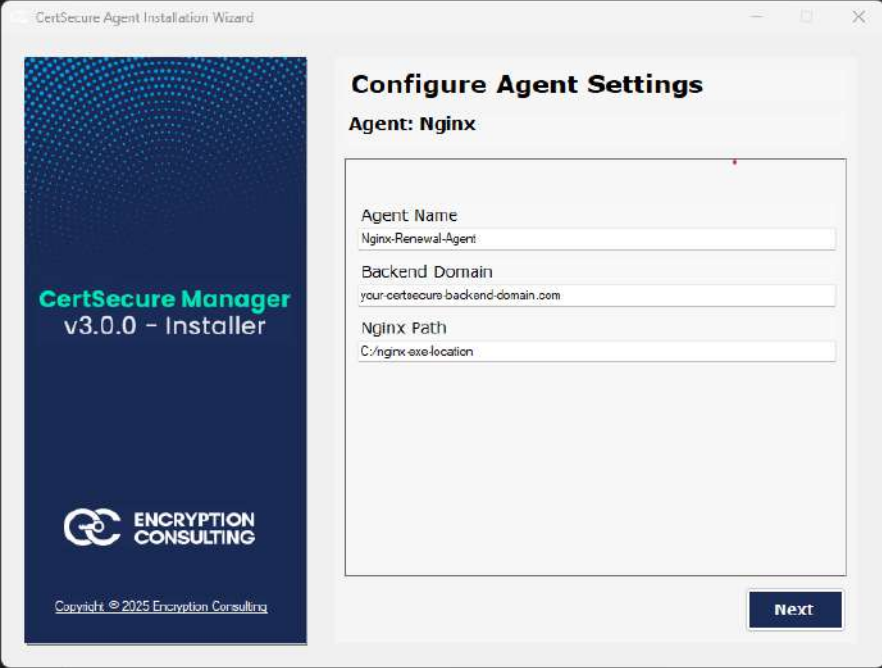
Run the Renewal agent installer as an administrator and choose the Nginx renewal agent for installation.



Steps:

Step 1: Mention the required details

- Provide a unique name for the agent.
- Provide the URL for your CertSecure Manager backend.
- Provide the path to the folder where nginx.exe is present on your system.

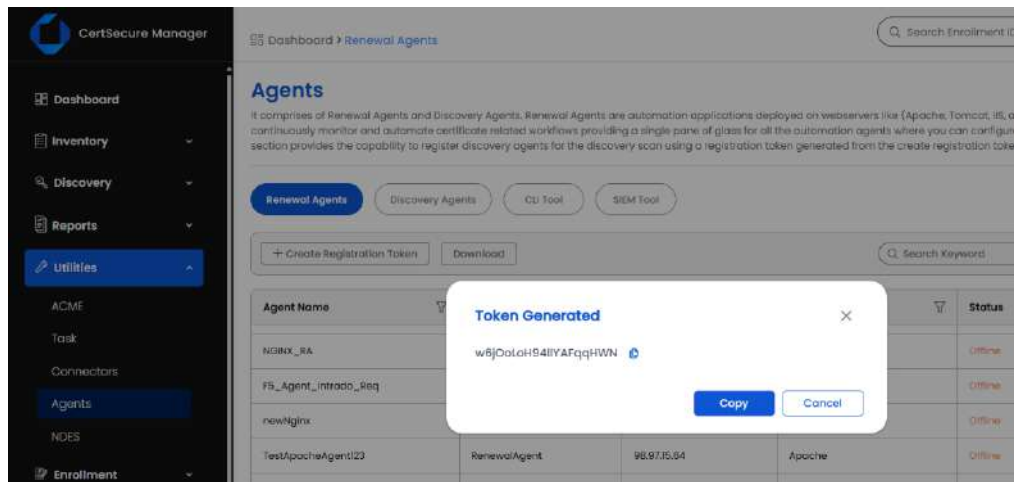


The screenshot shows the 'CertSecure Agent Installation Wizard' window. On the left is a dark blue sidebar with the text 'CertSecure Manager v3.0.0 - Installer' and the 'ENCRYPTION CONSULTING' logo. The main area is titled 'Configure Agent Settings' and 'Agent: Nginx'. It contains three input fields: 'Agent Name' with the value 'Nginx-Renewal-Agent', 'Backend Domain' with the value 'your-certsecure-backend-domain.com', and 'Nginx Path' with the value 'C:/nginx.exe-location'. A 'Next' button is located at the bottom right of the main area.

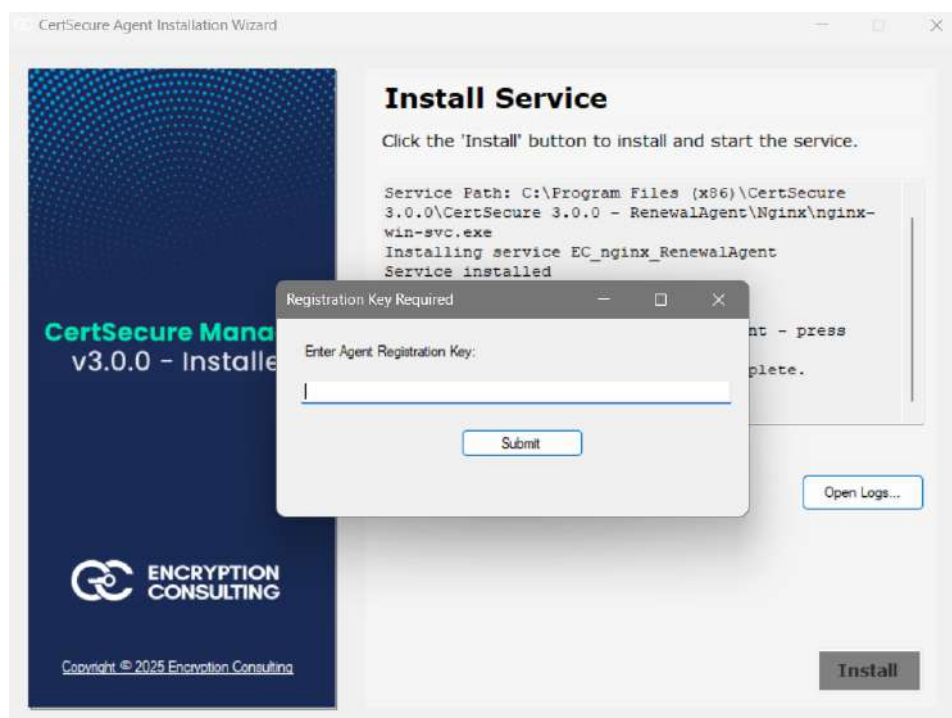
Field	Value
Agent Name	Nginx-Renewal-Agent
Backend Domain	your-certsecure-backend-domain.com
Nginx Path	C:/nginx.exe-location

Step 2: Register and run the agent

- On the CertSecure Manager UI, go to Utilities → Agents and then click on Create Registration token.



- Provide the registration token when the installer prompts to do so.



- Wait for the installer to finalise the installation and then close the installer.

Validation

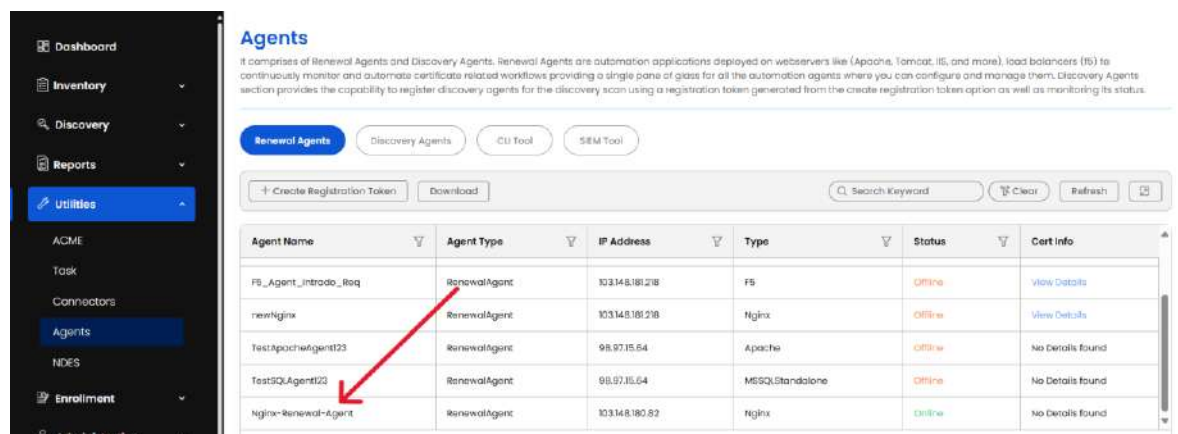
After the installation has finished, you can validate the installation by following these steps:

1. Validation

Steps:

Step 1: Validate

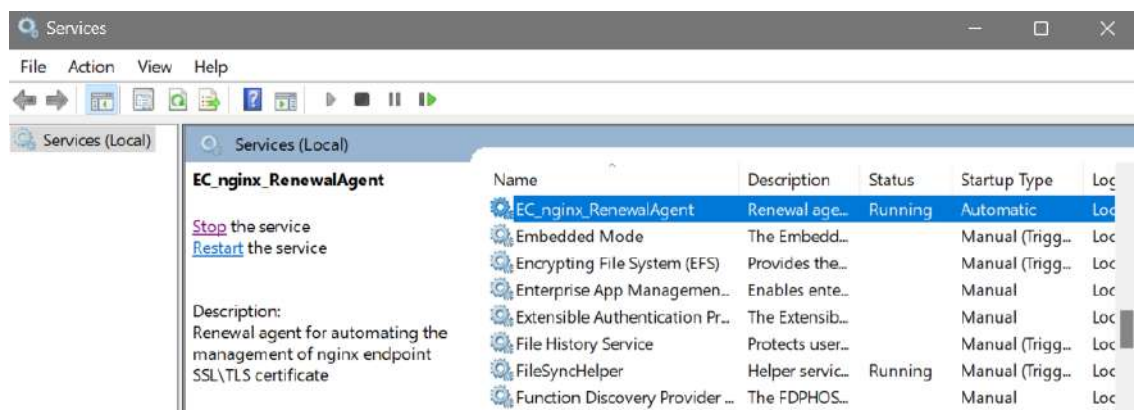
- On the CertSecure Manager UI, go to Utilities → Agents. You can see a renewal agent with the name provided during installation.



The screenshot shows the CertSecure Manager UI. The left sidebar has a menu with 'Utilities' selected, which has a sub-menu 'Agents'. The main content area shows a table of agents. A red arrow points to the 'nginx-Renewal-Agent' row.

Agent Name	Agent Type	IP Address	Type	Status	Cert Info
FB_Agent_introdo_Req	RenewalAgent	10.3.14.8.181.218	FS	Offline	View Details
newNginx	RenewalAgent	10.3.14.8.181.218	Nginx	Offline	View Details
TestApacheAgent23	RenewalAgent	98.97.15.64	Apache	Offline	No Details found
TestSQLAgent23	RenewalAgent	98.97.15.64	MSSQLStandalone	Offline	No Details found
nginx-Renewal-Agent	RenewalAgent	10.3.14.8.180.82	Nginx	Online	No Details found

- On the target machine, run services.msc and look for EC_Nginx_Renewal_Agent, you can monitor and manage the renewal agent from here.



The screenshot shows the Windows Services console. The 'EC_Nginx_RenewalAgent' service is selected and highlighted in blue. The service is running and has an automatic startup type.

Name	Description	Status	Startup Type	Log
EC_Nginx_RenewalAgent	Renewal age...	Running	Automatic	Loc
Embedded Mode	The Embedd...		Manual (Trigg...	Loc
Encrypting File System (EFS)	Provides the...		Manual (Trigg...	Loc
Enterprise App Managemen...	Enables ente...		Manual	Loc
Extensible Authentication Pr...	The Extensib...		Manual	Loc
File History Service	Protects user...		Manual (Trigg...	Loc
FileSyncHelper	Helper servic...	Running	Manual (Trigg...	Loc
Function Discovery Provider ...	The FDPHOS...		Manual	Loc

- You can also monitor the agent logs by accessing the log file at **C:/CertSecure/logs**

