

Prerequisites:

To get the F5 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.

2. F5 Account with Advanced Shell access

To set up the renewal agent you also need a F5 account with advanced shell access permission.

Steps:

Step 1: Navigate to the User List

- Login to F5 as an Admin.
- On the left sidebar, click on System.
- Go to Users and then User List.

Step 2: Create an account with the required permissions

- Provide the required details and select Advanced Shell from the dropdown menu for Terminal Access and click on Finished.

System >> Users : User List >> New User...

Account Properties

User Name: test-user

Password: New: [masked], Confirm: [masked]

Role: Administrator

Partition: All

Add

Role	Partition
Administrator	[All]

Edit Delete

Terminal Access: Advanced shell

Disabled
Advanced shell
tmsh

Cancel Repeat Finished

3. 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.

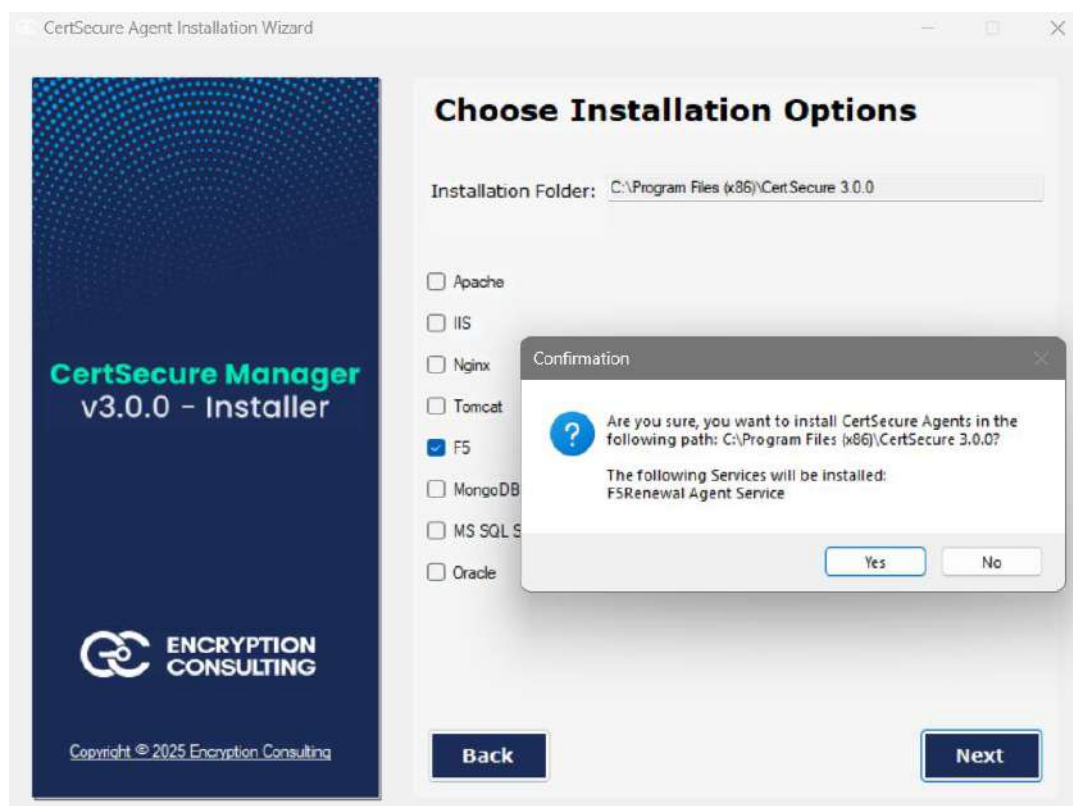
You must also be able to SSH into your deployed F5 instance from the target machine; therefore, ensure that port 22 is open and accessible.

Installation

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

1. Configuration and Installation

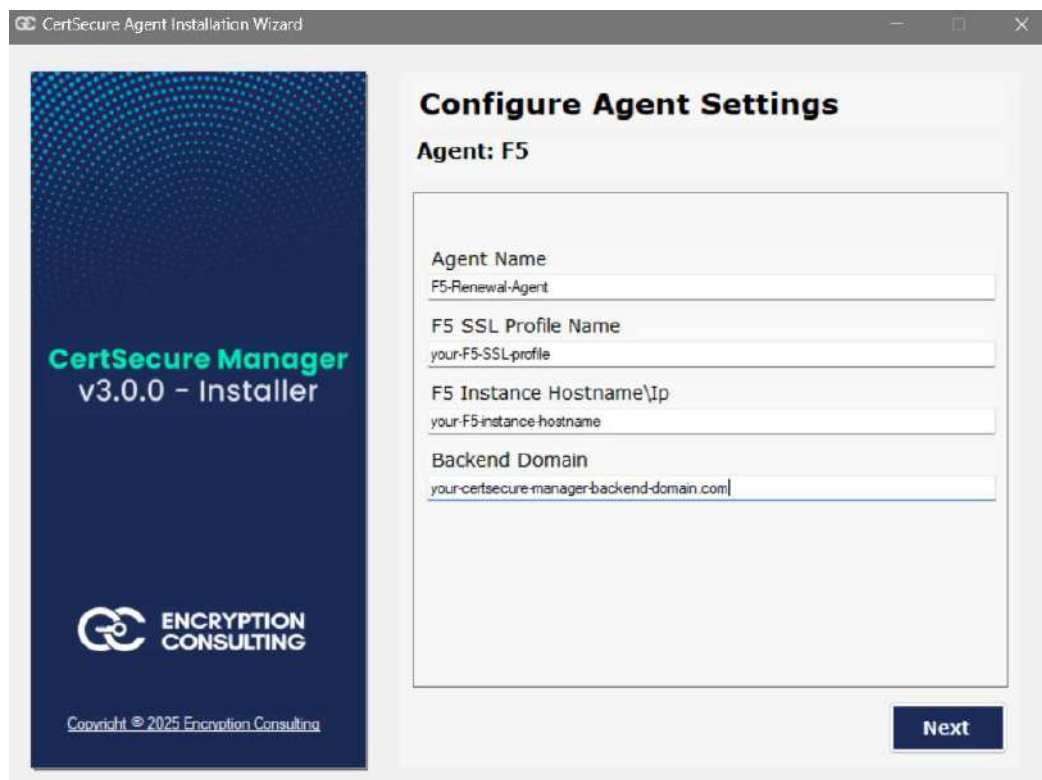
Run the Renewal agent installer as an administrator and choose the F5 renewal agent for installation.



Steps:

Step 1: Mention the required details

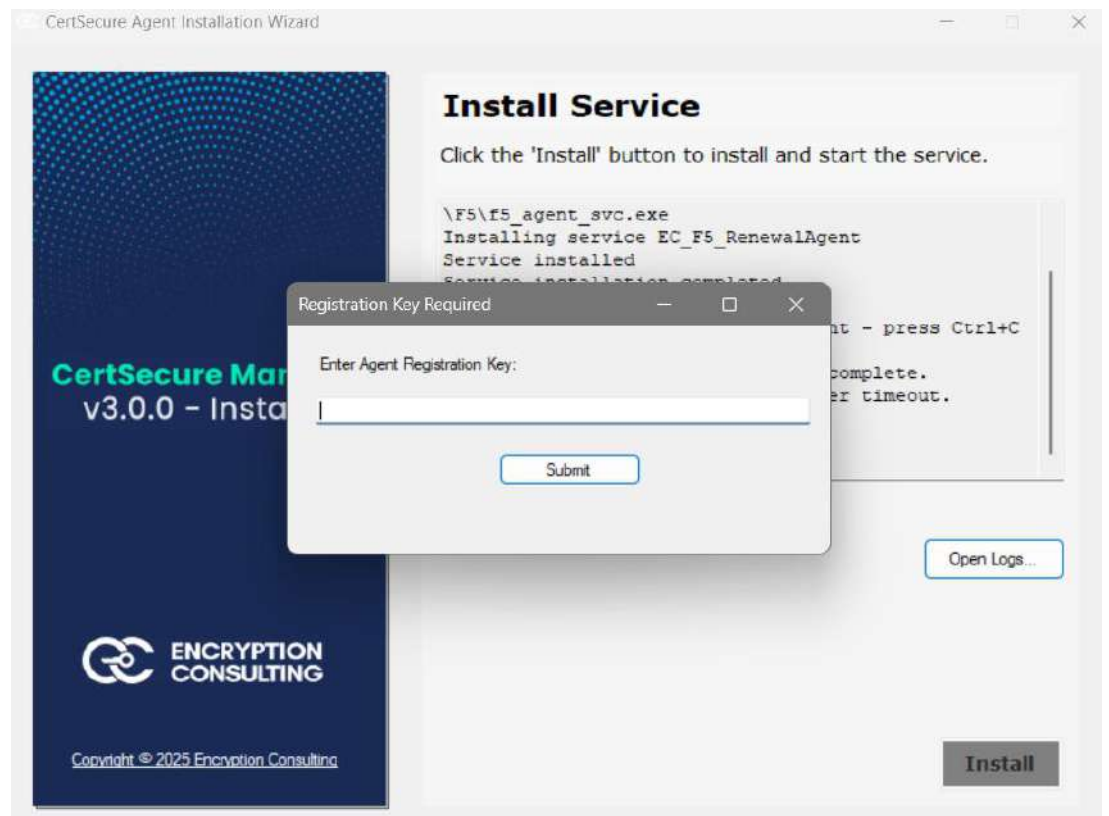
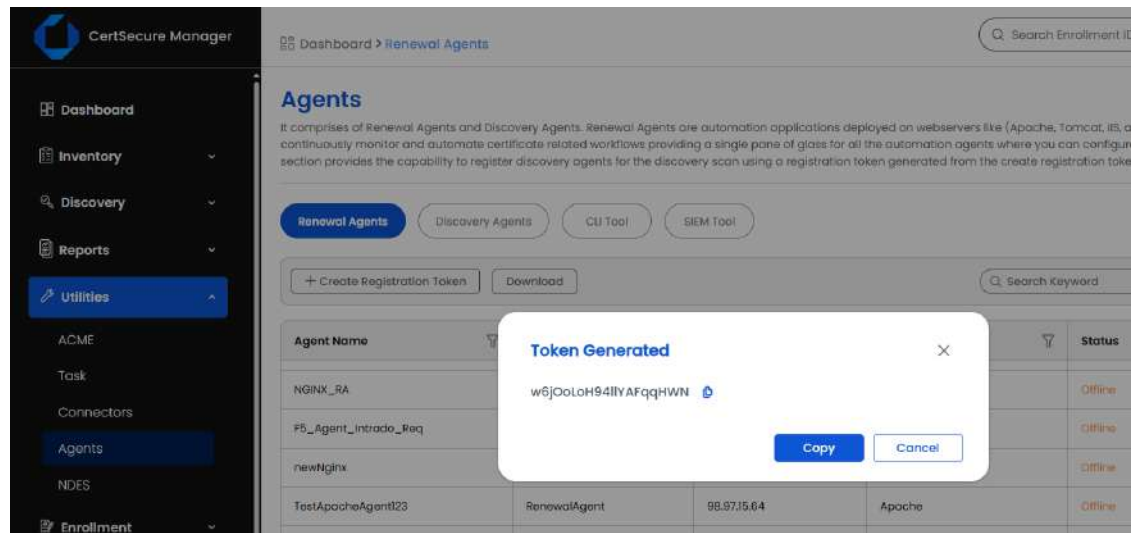
- Provide a unique name for the agent.
- Provide the desired F5 SSL profile name to which you want the certificate to be bound.
- Provide the hostname/IP address of your deployed F5 instance.
- Provide the URL for your CertSecure Manager backend.



The screenshot shows a window titled "CertSecure Agent Installation Wizard". 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: F5". It contains four input fields: "Agent Name" (with placeholder "F5-Renewal-Agent"), "F5 SSL Profile Name" (with placeholder "your-F5-SSL-profile"), "F5 Instance Hostname\Ip" (with placeholder "your-F5-instance-hostname"), and "Backend Domain" (with placeholder "your-certsecure-manager-backend-domain.com"). A "Next" button is at the bottom right.

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.
- Now mention the F5 account credentials.
- Wait for the installer to finalise the installation and then close the installer.



Validation

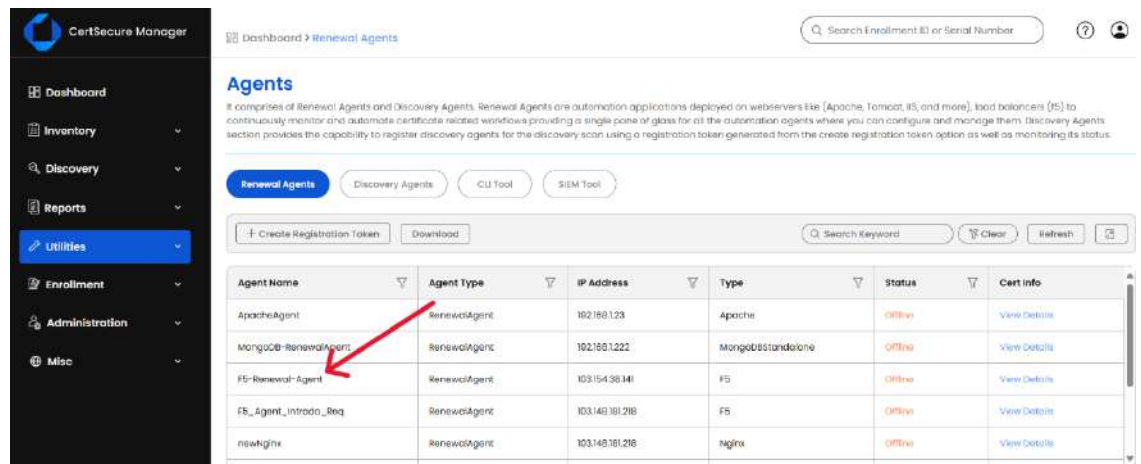
After the installation has finished, you can validate the installation by following these steps:

1. Validation

Steps:

Step 1: Validate

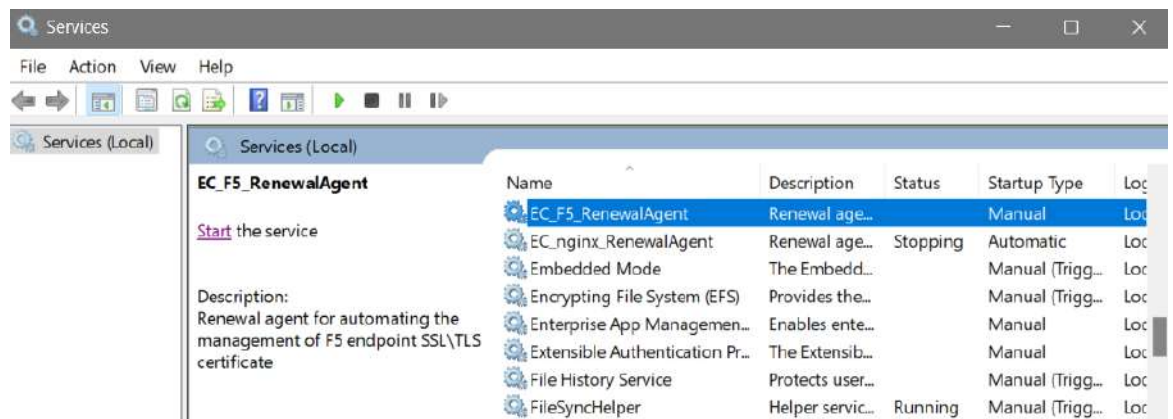
- On the CertSecure Manager UI, go to Utilities → Agents. You can see a renewal agent with the name provided during installation.



The screenshot shows the CertSecure Manager web interface. The left sidebar contains a 'Utilities' menu item. The main content area is titled 'Agents' and displays a table of registered agents. A red arrow points to the 'F5-Renewal-Agent' row in the table.

Agent Name	Agent Type	IP Address	Type	Status	Cert Info
ApacheAgent	RenewalAgent	192.168.1.23	Apache	Offline	View Details
MongoDB-RenewalAgent	RenewalAgent	192.168.1.222	MongoDBStandalone	Offline	View Details
F5-Renewal-Agent	RenewalAgent	103.154.38.141	F5	Offline	View Details
F5_Agent_Intrada_Req	RenewalAgent	103.149.161.298	F5	Offline	View Details
nginx	RenewalAgent	103.149.161.298	nginx	Offline	View Details

- On the target machine, run services.msc and look for EC_F5_Renewal_Agent, you can monitor and manage the renewal agent from here.



The screenshot shows the Windows Services console. The 'Services (Local)' list on the right includes the 'EC_F5_RenewalAgent' service, which is highlighted. The left pane shows the 'Start' button and the description: 'Renewal agent for automating the management of F5 endpoint SSL/TLS certificate'.

Name	Description	Status	Startup Type	Log
EC_F5_RenewalAgent	Renewal age...	Stopping	Manual	Loc
EC_nginx_RenewalAgent	Renewal age...	Automatic	Automatic	Loc
Embedded Mode	The Embedd...	Manual (Trigg...	Manual (Trigg...	Loc
Encrypting File System (EFS)	Provides the...	Manual (Trigg...	Manual (Trigg...	Loc
Enterprise App Managemen...	Enables ente...	Manual	Manual	Loc
Extensible Authentication Pr...	The Extensib...	Manual	Manual	Loc
File History Service	Protects user...	Manual (Trigg...	Manual (Trigg...	Loc
FileSyncHelper	Helper servic...	Running	Manual (Trigg...	Loc

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