

JKS Integration Guide

This guide outlines the steps to install, configure, and use the CertSecure CLI Agent for managing certificates, integrating with Java KeyStore (JKS), and enabling automated certificate rotation.

Prerequisites

Before proceeding, ensure the following:

- You have downloaded the latest `certsecure_cli_agent.exe` and `configure.exe`.
- The IP address or hostname of the CertSecure Backend server is known and reachable.
- Java Runtime Environment (JRE) is installed (for JKS-related operations).
- Necessary network ports are open for agent-backend communication (default: 443/HTTPS).
- On Windows, administrative rights may be required for configuration and JKS file access.

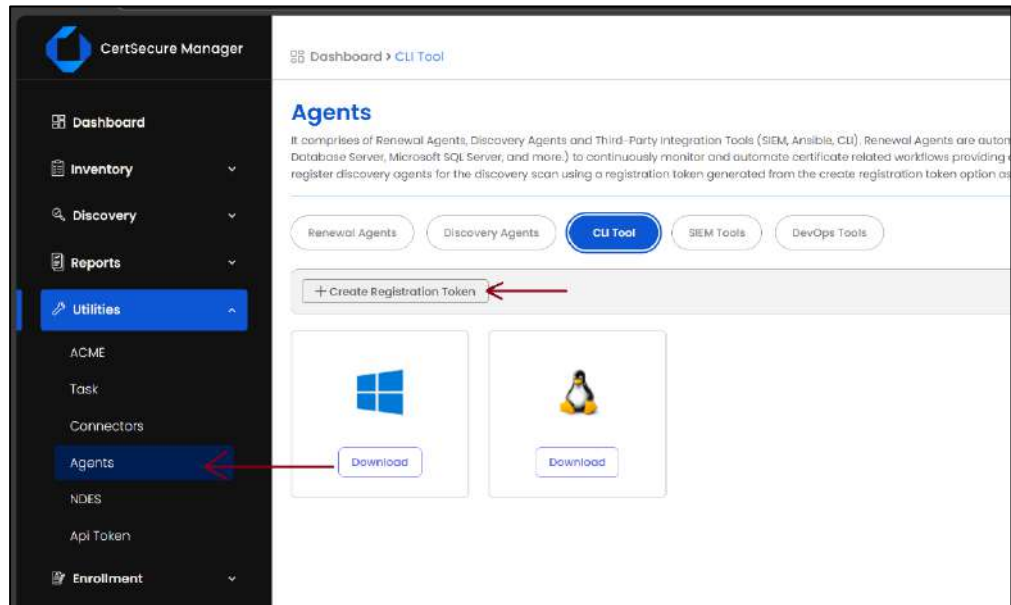
Step 1: Download and Extract the Agent

1. Download `certsecure_cli_agent.exe` and `configure.exe` from the official CertSecure distribution.
2. Move both files to a working directory of your choice.
3. Ensure execution permissions if required (especially on non-Windows systems using Wine or similar).

Step 2: Configure the Agent

1. Run the configuration tool:
 - **`./configure.exe`**
2. Follow on-screen prompts to complete setup:
 - Server IP Address – IP of the CertSecure Backend.
 - Registration Token –
A valid registration token is available from the CertSecure Manager UI portal.

- Click on “Create Registration Token.” → Copy the token and paste it in the CLI agent console.



- Base Directory – Path where the downloaded certificates should be stored.

Note: Configuration is stored persistently and only needs to be completed once unless changes are required.

Step 3: Use the CLI Agent

1. Launch the agent:
 - **certsecure_cli_agent.exe**
2. Available operations:
 - Request and download certificates
 - View certificate metadata
 - Integrate certificates into a Java KeyStore (JKS)
 - Push CA certificates into JKS
 - Enable automated certificate renewal (rotation)

Step 4: Java KeyStore (JKS) Integration

During CLI usage:

1. When prompted:
 - Provide the path to the target JKS file
 - Enter the JKS password
2. The CLI agent will:
 - Insert the downloaded certificate(s)
 - Push CA certificates for establishing trust

Step 5: Manage Certificate Rotation

1. Use the CLI interface to enable auto-renewal.
2. The agent will monitor expiration dates and trigger renewals automatically.

Step 6: Reconfigure the Agent (If needed)

To update the saved configuration:

- **`./configure.exe`**

Step 7: Connectivity Requirements

1. Ensure outbound HTTPS connectivity from the agent system to the CertSecure Backend.
2. If firewalls are enabled:
 - Open required ports (typically 443)
 - Allow the agent executable through security rules
3. Ensure proxies or SSL interception mechanisms do not block agent communication.