JKS Discovery Integration Guide

This guide describes how to discover and inventory Java KeyStore (JKS) files in CertSecure Manager using a Discovery Agent.

Prerequisites

A system administrator must:

- Have the Manage Discovery permission in CertSecure Manager.
- Have a Discovery Agent installed and showing as Online.
- Know the location of the keystores to be scanned (folder or file path).
- For keystores on Windows machines: the agent must be running on Windows. If the keystore is on a different machine, the folder must be shared, and the agent's service account must have read access to it.
- For keystores on Linux servers: SSH access on port 22, with a username and password for each server.

Note: The keystore password is not required. CertSecure can inventory a keystore without it.

Integration Steps

Step 1: Create the Scan Configuration

- Log in to the CertSecure Manager portal.
- Navigate to Discovery > Scans.
- Click Create Scan.

Step 2: Select the Scan Type

- Scan Name: Provide a friendly name for internal reference.
- Scan Type: Select Store.
- Store Type: Select JKS.

Step 3: Select the Target

Choose where the keystores are located:

- Windows - No host list is required. The agent reads the paths directly.
- Linux - Add each server with its Host, Username, and Password. Alternatively, enable Discover Hosts to find them automatically.

Step 4: Enter the Keystore Paths

The Paths field is pre-filled with the common Java keystore locations. Edit, add, or remove entries as needed. Files and folders can be mixed in the same list.

To Scan	Enter
One keystore	C:\Keystores\keystore.jks
A keystore on another Windows machine	\\SERVER01\Keystores\keystore.jks
An entire folder	C:\Keystores
Common Linux locations	/opt, /usr/lib/jvm

Note: A folder is searched; a file is opened directly.

Step 5: Complete the Remaining Fields

- Keystore Password: Optional. Leave blank unless the keystore requires one.
- Owner or Watcher Group: Select who receives notifications.
- Enable Expiry Alerts and the Completion Report if required.
- Click Save.

Step 6: Run the Scan

- Locate your scan in the Discovery > Scans list.
- Click Run.
- Select an Agent from the dropdown.
- Choose Run Now, or set a date, time, and interval to schedule it.
- Click Submit.

Step 7: View the Results

- Navigate to Discovery > Inventory.
- Results are grouped one row per keystore file. Expand a row to see every certificate inside, each listed with its Alias and Chain Position.

A single keystore commonly contains several certificates - the server certificate, its issuing CA certificates, and any trusted roots. This is expected.

The scan record lists every location that was searched, so an empty result confirms those locations held no keystores.

Troubleshooting

Issue	Resolution
Agent cannot be selected	The agent must be Online, and running on Windows for C:\ or \\server\ paths.
Scan completes with no certificates	Open the scan log and review the searched locations. The path may be incorrect, or the agent may not have read access to the shared folder.
Keystore on another Windows machine not found	A path beginning C:\ always refers to the agent's own drive. Use the \\machine\share\... format instead.