AAP Integration Guide

CertSecure Manager integrates with Ansible Automation Platform (AAP) so you can launch certificate deployment and renewal automation - via Ansible playbooks - directly from CertSecure, with every job tracked alongside the rest of your certificate inventory.

Prerequisites

- CertSecure Manager deployed and reachable, with an account that has permission to configure integrations (Integration → DevOps).
- Ansible Automation Platform 2.4 or later, with the controller reachable from the CertSecure Manager backend over HTTPS.
- An AAP user or service account with permission to create projects, inventories, and job templates in the target organization, plus the AAP Organization ID.
- A Personal Access Token (PAT) generated in AAP for that account - required for AAP 2.5+ and recommended for earlier versions.
- The AAP controller's TLS trust material on hand (PEM trust bundle) if the controller uses a private or internal CA.
- Target hosts already registered in AAP, with working SSH/WinRM credentials and the privileges needed to write certificates and restart the affected service.
- Outbound network access from the target hosts to the ACME endpoint that will issue the certificates (CertSecure's internal ACME service, or the public CA).
- DNS-01 provider credentials available if public issuance will be used for domains requiring DNS validation.

Step 1: Prepare Certificate Issuance

Before connecting AAP, decide how the playbooks will obtain certificates:

- For private issuance (default): generate an ACME enrollment profile under Settings → ACME, so the playbook can request certificates from CertSecure's own ACME server.
- For public issuance (e.g. Let's Encrypt): add the public CA's ACME URL under Settings → ACME → Add CA URL, and configure DNS-01 provider credentials if the domain requires it.

Step 2: Open the AAP Utility

- Go to: Integration → DevOps → Automation Platform (AAP).

Step 3: Add an AAP Connection

- Click Add Connection in the top right.

Step 4: Configure the Connection

- **Name:** a name to identify this AAP instance.
- **Base URL:** the AAP controller URL (e.g. https://aap.certsecure.com). Must be reachable from the CertSecure Manager backend.
- **Organization ID:** the AAP organization this connection operates under.
- **Personal Access Token:** paste the PAT (recommended for AAP 2.5+, since the split-gateway architecture no longer exposes the classic OAuth2 token endpoint).
- **TLS Verification:** System / Custom Bundle / Insecure. If Custom Bundle, paste the trust bundle (PEM).

Note: CertSecure tests reachability, authentication, and capability against AAP before saving the connection. On success, it automatically provisions a project named "CertSecure" in your AAP organization - no manual project setup is required.

Step 5: Set Up Inventory and Hosts

- Under the connection, go to Inventories.
- Select an existing AAP inventory, or create a new one.
- Add the target hosts that certificates will be deployed to or renewed on.

Note: Inventories and hosts live in AAP - CertSecure does not cache them, so add/update hosts in AAP if they change.

Step 6: Create or Onboard a Job Template

Under the connection, go to Job Templates, then choose one:

- **Create New** - build a template against the auto-provisioned CertSecure project:
  - Name: a name for the new job template.
  - Inventory: the inventory from Step 5.
  - Playbook: select the target type - nginx, Apache, IIS, Tomcat, MongoDB, MS SQL Server, Oracle, or Custom (fully variable-driven).
  - Extra Variables (optional): default values such as common_name, subject_alt_names, acme_flow (private/public), key_type/key_size.
  - Description (optional).
- **Onboard Existing** - pick a job template a platform engineer already built directly in AAP.

Note: Only job templates created or onboarded through CertSecure can be launched from CertSecure - this keeps CertSecure as a consumer of automation, not an author of it in AAP directly.

Step 7: Launch or Schedule a Job

Click Launch on a job template to run it now, or Schedule to run it on a recurring basis.

- **Launch Now:** choose the connection and job template, optionally override Extra Variables, and target either a single host/limit pattern or a batch of hosts.
- **Schedule:** choose Simple (frequency, interval, start date/time) or Advanced (a raw recurrence rule) for recurring renewal runs.

Step 8: Track Job Status

- Launched jobs appear on the Tasks page and under the connection's Jobs view, showing status per host for batch runs.

Note: For public-CA issuance flows, ensure the corresponding ACME CA URL and DNS provider credentials from Step 1 are still valid - expired or misconfigured DNS credentials will cause the playbook run to fail at the certificate-request step.