CertSecure ServiceNow Integration Guide

STEP 1: Prepare Your ServiceNow Instance

1. Login to your **ServiceNow instance** with admin-level permissions.
2. Ensure you have an **active REST endpoint** or are ready to accept **API POST requests** from CertSecure.
3. (Optional but recommended) Create a dedicated integration user:
    - Navigate to **User Administration → Users**
    - Create a new user (e.g., certsecure.api)
    - Assign appropriate roles (e.g., web_service_admin, or a custom role with access to create and update incidents or custom tables)

STEP 2: Collect Required Connection Details

You will need the following information from your ServiceNow instance:

- **Instance URL**: The full URL of your instance, e.g., https://your-instance.service-now.com
- **Username**: The username of the integration user (or admin account)
- **Password**: The password for the integration user

Keep this information secure and ready for input in CertSecure.

STEP 3: Configure ServiceNow Integration in CertSecure

1. Login to **CertSecure Manager** (Admin Portal).
2. Navigate to: **Misc → Service Setup → ServiceNow**
3. Fill in the required fields:
    - **Instance URL***: Paste your ServiceNow instance URL (e.g., https://your-instance.service-now.com)

- **Username***: Enter the username for your integration account
- **Password***: Enter the corresponding password

4. Click **Save**.

STEP 4: Validate the Integration

CertSecure will immediately attempt to connect to your ServiceNow instance using the provided credentials.

- A **test request** is sent to validate API connectivity and authentication.
- If successful, a confirmation message will appear:
  "Connection Successful"

STEP 5: Automate Certificate-Based Ticketing

Once the integration is validated, CertSecure will start automatically creating or updating ServiceNow tickets for certificate-related events. This may include:

- Certificates that are about to **expire**
- Certificates that have been **revoked**
- **Failures** in renewal or enrollment processes
- Any other alert conditions configured in CertSecure

Tickets will include contextual information such as:

- Certificate name or common name (CN)
- Serial number
- Owner (if available)
- Event type and timestamp
- Suggested remediation or action