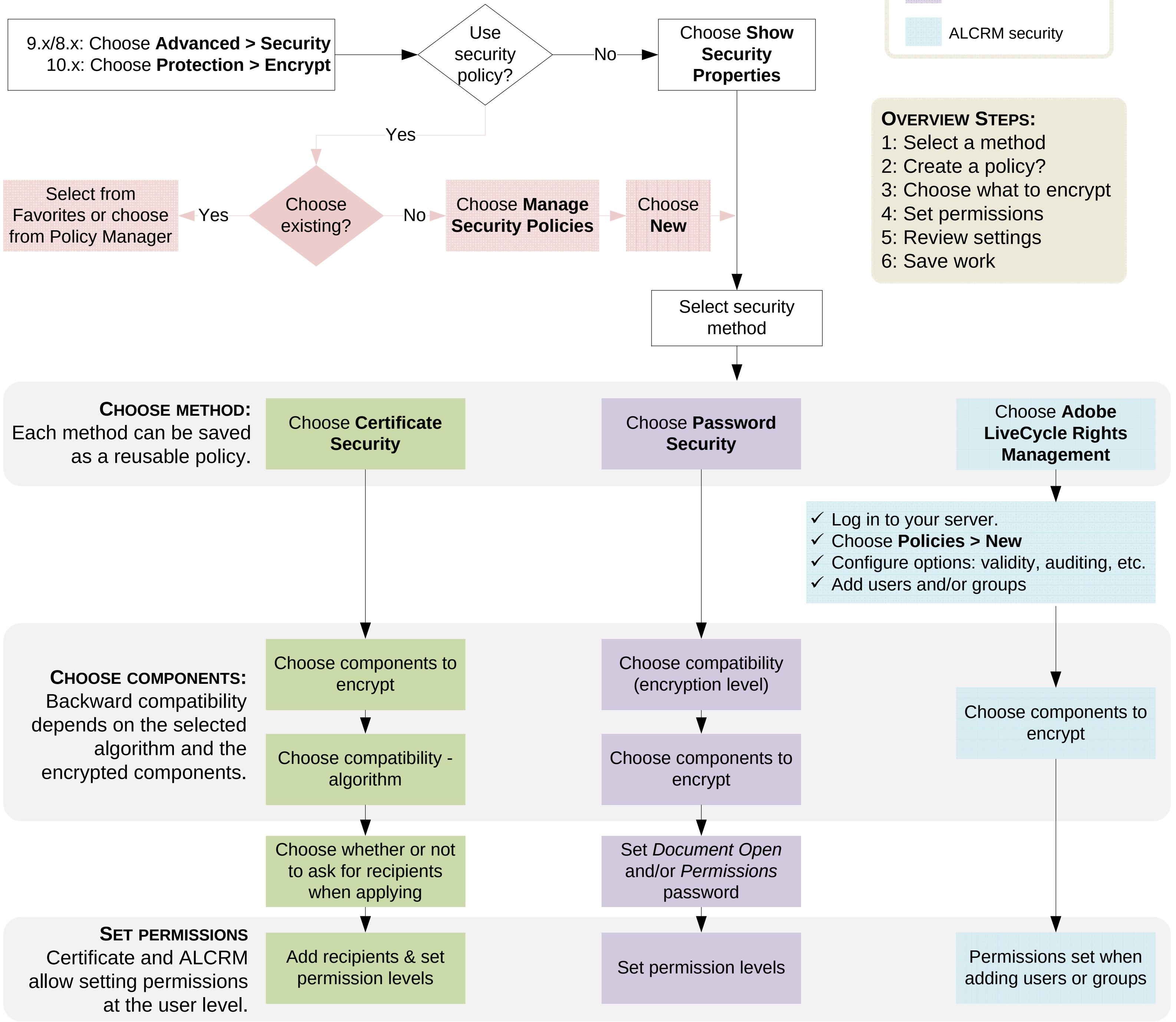
Security Methods: setting encryption levels and permissions

KEY

- 🟥 Policy workflow
- 🟩 Certificate security
- 🟪 Password security
- 🟦 ALCRM security



9.x/8.x: Choose **Advanced > Security**
10.x: Choose **Protection > Encrypt**

Use security policy?

No → Choose **Show Security Properties**

Yes → Choose existing?

Yes → Select from Favorites or choose from Policy Manager

No → Choose **Manage Security Policies** → Choose **New**

Select security method

Overview Steps:
1: Select a method
2: Create a policy?
3: Choose what to encrypt
4: Set permissions
5: Review settings
6: Save work

Choose method: Each method can be saved as a reusable policy.

Choose **Certificate Security**

Choose **Password Security**

Choose **Adobe LiveCycle Rights Management**

- ✓ Log in to your server.
- ✓ Choose **Policies > New**
- ✓ Configure options: validity, auditing, etc.
- ✓ Add users and/or groups

Choose components: Backward compatibility depends on the selected algorithm and the encrypted components.

Choose components to encrypt → Choose compatibility - algorithm → Choose whether or not to ask for recipients when applying → Add recipients & set permission levels

Choose compatibility (encryption level) → Choose components to encrypt → Set *Document Open* and/or *Permissions* password → Set permission levels

Choose components to encrypt → Permissions set when adding users or groups

Set permissions Certificate and ALCRM allow setting permissions at the user level.

Pros:
- ✓ No password to remember.
- ✓ Key not susceptible to brute force discovery and resides only on the recipients machine.
- ✓ Can encrypt documents for specific people.
- ✓ Can use certificates from trusted 3rd party.
- ✓ Specifies different permissions for users.
- ✓ Leverages LDAP for recipients & groups.

Cons:
- ✓ Users must have a digital ID.
- ✓ Requires distributing/managing digital IDs.
- ✓ Full support appears first in 6.0.

Pros:
- ✓ Backward-compatible to Acrobat 3.0 for certain encryption levels.
- ✓ Simple and easily understood.
- ✓ Share documents by sharing the password.
- ✓ Different open & permission password.

Cons:
- ✓ Password strength is critical.
- ✓ Users share the same permissions.
- ✓ Disabled when in FIPS mode.

Pros:
- ✓ Centralized policy administration.
- ✓ Document auditing.
- ✓ Allows setting permissions for separate tasks such as opening, editing, and so on.
- ✓ Can specify different permissions for users.
- ✓ Leverages LDAP for recipients & groups.
- ✓ Offline control: Can specify a validity time limit after which document expires and is locke

Cons:
- ✓ Requires a network connection, an administrator, and a LiveCycle Server.