

# Clango Retriever Deployment Guide



**Version 1.0.0**

**Jan 2021**

**Prepared by:**



## Contents

1	Overview .....	1
2	Download License Files .....	1
3	License Installation.....	1
4	Configure Access .....	4
4.1	Configure Users.....	4
4.2	Configure Password Visibility.....	5
4.3	Configure Search Properties .....	6
5	Install Retriever on User Workstations.....	6
5.1	Manual Installation .....	6
5.1.1	Chrome.....	6
5.1.2	Edge.....	7
5.1.3	Firefox .....	8
5.2	Automatic Installation.....	8
5.2.1	Chrome.....	8
5.2.2	Edge.....	9
5.2.3	Firefox .....	10
6	Configure Retriever on User Workstations.....	10

## 1 Overview

This guide provides instructions for deploying Clango Retriever for your organization. The deployment consists of these main steps:

1. Request and download the Clango Retriever license and installation files
2. Install license files
3. Configure access
4. Install browser extension on end users' workstations
5. Configure browser extension on end users' workstations

## 2 Download License Files

To obtain a download link for the Clango Retriever license files, fill out and submit the Clango Retriever request form located here: <https://clango.com/request-download-clango-retriever/>

The download link will contain a trial license and, if requested, the XPI file for installing in Firefox.

## 3 License Installation

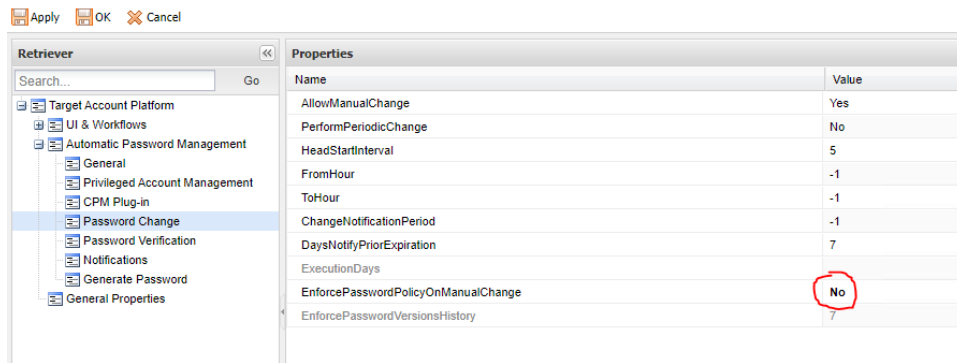
Clango will provide three files related to the license: a license key, a company public key, and a client private key. All three must be installed in the vault for end users to use the extension. The keys will be installed by creating a new safe with three accounts, one for each key, set up as detailed below.

1. In PVWA, create a new safe called **Clango-Retriever**.
  - a. Leave **Enable Object Level Access Control** unchecked.
  - b. For **Assigned to CPM**, choose **[None]**.

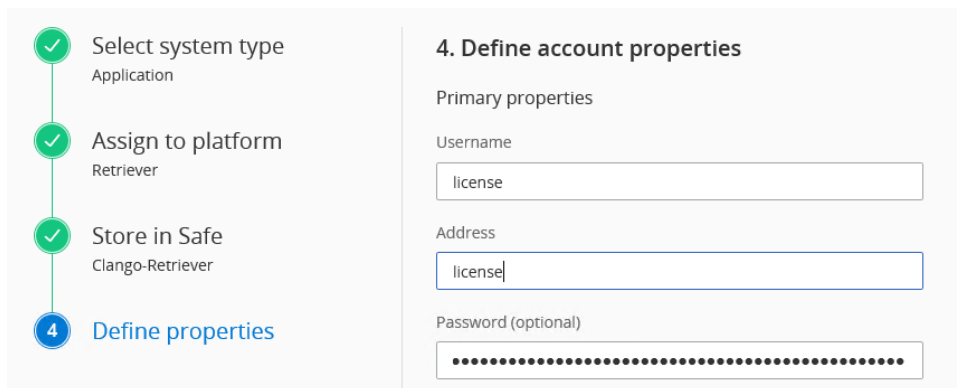
### Add Safe

Safe name:	<input type="text" value="Clango-Retriever"/>
Description:	<input type="text"/>
	<input type="checkbox"/> Enable Object Level Access Control
Saved accounts:	<input type="radio"/> Save the last <input type="text" value="5"/> account versions
	<input checked="" type="radio"/> Save account versions from the last <input type="text" value="7"/> days
Assigned to CPM:	<input type="text" value="[None]"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

2. Create a new account.
  - a. Use **Application** for the system type.
  - b. Select a platform that does not enforce a password policy. If none exists, create one.
    - i. Ensure that the **AllowedSafes** regular expression under **Automatic Password Management > General** for the platform will validate **Clango-Retriever** (e.g., **.\*** or **Clango.\***).
    - ii. To configure a platform to not enforce a password policy, in the Administration > Platform Management module, modify the **EnforcePasswordPolicyOnManualChange** property to **No** under **Automatic Password Management > Password Change** for the platform.



- c. Choose the **Clango-Retriever** safe.
- d. Enter “license” for both username and address.
- e. For the password field, enter the contents of the provided file license.properties.



3. Create another new account.
  - a. Use **Application** for the system type.
  - b. Select the same platform you chose in step 2.
  - c. Choose the **Clango-Retriever** safe.
  - d. Enter “company-public-key” for both username and address.
  - e. For the password field, enter the contents of the provided file company-public.pub.

The screenshot displays a vertical progress bar on the left with four steps: 1. Select system type (Application), 2. Assign to platform (Retriever), 3. Store in Safe (Clango-Retriever), and 4. Define properties (highlighted in blue). The main content area is titled "4. Define account properties" and includes a "Primary properties" section with three input fields: "Username" (containing "company-public-key"), "Address" (containing "company-public-key"), and "Password (optional)" (filled with dots).

4. Create another new account.
  - a. Use **Application** for the system type.
  - b. Select the same platform you chose in step 2.
  - c. Choose the **Clango-Retriever** safe.
  - d. Enter “client-private-key” for both username and address.
  - e. For the password field, enter the contents of the provided file client-private.key.

The screenshot displays a vertical progress bar on the left with four steps: 1. Select system type (Application), 2. Assign to platform (Retriever), 3. Store in Safe (Clango-Retriever), and 4. Define properties (highlighted in blue). The main content area is titled "4. Define account properties" and includes a "Primary properties" section with three input fields: "Username" (containing "client-private-key"), "Address" (containing "client-private-key"), and "Password (optional)" (filled with dots).

5. Verify you have added the license, client-private-key, and client-public-key accounts:

☆	Status	Username	Address	Platform ID
☆	⚡	client-private-key	client-private-key	Retriever
☆	⚡	company-public-key	company-public-key	Retriever
☆	⚡	license	license	Retriever

## 4 Configure Access

### 4.1 Configure Users

Users of Retriever must be granted access to the **Clango-Retriever** safe in PVWA with the **Use Accounts, Retrieve Accounts** and **List Accounts** permissions granted.

#### Safe Details: Clango-Retriever

[Back](#)
[Edit](#)
[Delete Safe](#)
[Refresh](#)

[Add Safe](#)
[Customize](#)


Name: Clango-Retriever  
 Description: Object level access is not enabled  
 Assigned CPM: None  
 Saved accounts: Account versions from the last 7 days

The screenshot shows the 'Members' tab of the Clango-Retriever safe configuration. A red circle highlights the 'Add Member' button. Below the button is a table with the following columns: User Name, Use, Retri..., List, Add, Upd..., Upd..., CPM, Ren..., Delete, Unlock, Man..., and Vi. The table is currently empty.

**Add Safe Member**

Search:  Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 demouser1		Demo User1

Access

- Use accounts
- Retrieve accounts
- List accounts

Account Management

Safe Management

Monitor

- View Audit log
- View Safe Members

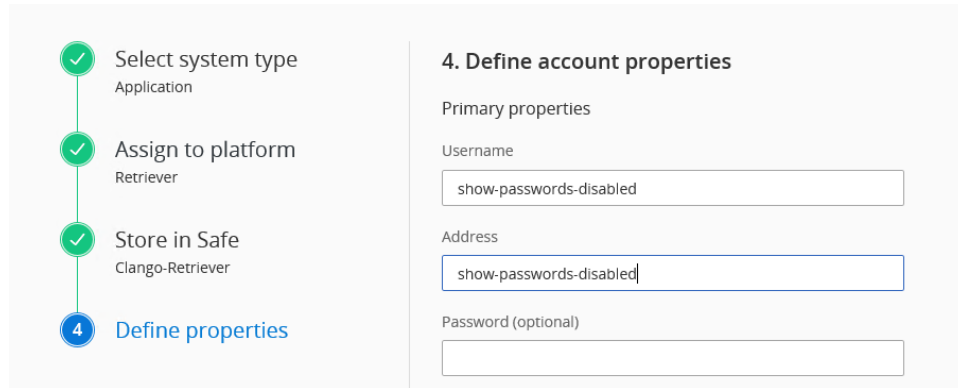
Workflow

## 4.2 Configure Password Visibility

If your organization chooses to disable displaying the retrieved password in the Retriever popup, an additional account must be created.

**Note: The password is still accessible to an end user when it is retrieved and placed in the password input on the HTML form.**

1. Create a new account.
  - a. Use **Application** for the system type.
  - b. Select the same platform you chose in License Installation step 2.
  - c. Choose the **Clango-Retriever** safe.
  - d. Enter “show-passwords-disabled” for both username and address.
  - e. For the password field, leave blank.



The screenshot shows a deployment wizard with a progress indicator on the left and a form on the right. The progress indicator has four steps: 1. Select system type (Application), 2. Assign to platform (Retriever), 3. Store in Safe (Clango-Retriever), and 4. Define properties (highlighted in blue). The form on the right is titled '4. Define account properties' and has a section for 'Primary properties' with three input fields: 'Username' (containing 'show-passwords-disabled'), 'Address' (containing 'show-passwords-disabled'), and 'Password (optional)' (empty).

### 4.3 Configure Search Properties

If your organization uses Business Users, you may need to update the search properties to include fields found on Business User accounts.

1. In PVWA, click **Administration > Configuration Options > Options > Search Properties**.
2. Right-click **Search Properties**, and then click **Add Property**. Add the following properties: itemname, url, tags, and notes.

## 5 Install Retriever on User Workstations

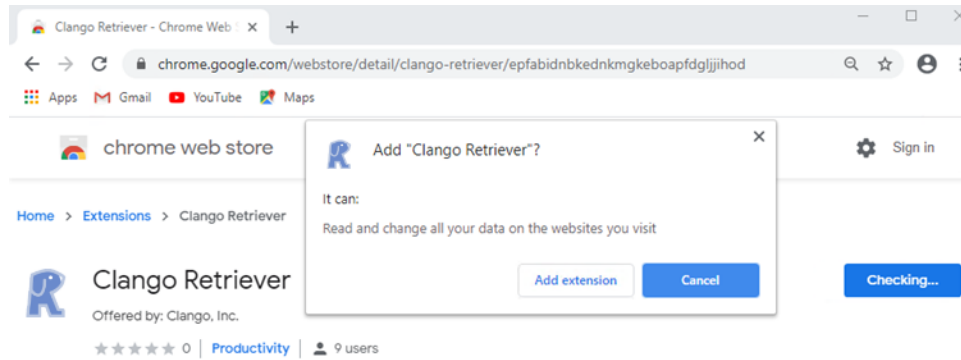
The browser extension can be installed on Google Chrome, Microsoft Edge, and Mozilla Firefox. The extension can be installed via the Chrome Web Store in both Chrome and Edge. In Firefox, end users need access to the XPI file provided by Clango.

### 5.1 Manual Installation

#### 5.1.1 Chrome

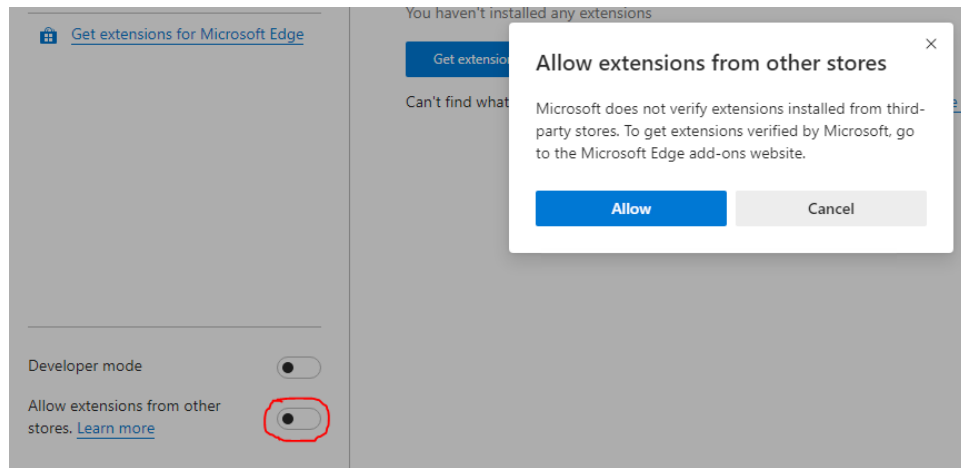
1. Navigate to <https://chrome.google.com/webstore/detail/clango-retriever/epfabidnbkednkmgkeboapfdgljjihod>.
2. Click **Add to Chrome**.
3. Click **Add extension** in the confirmation popup.



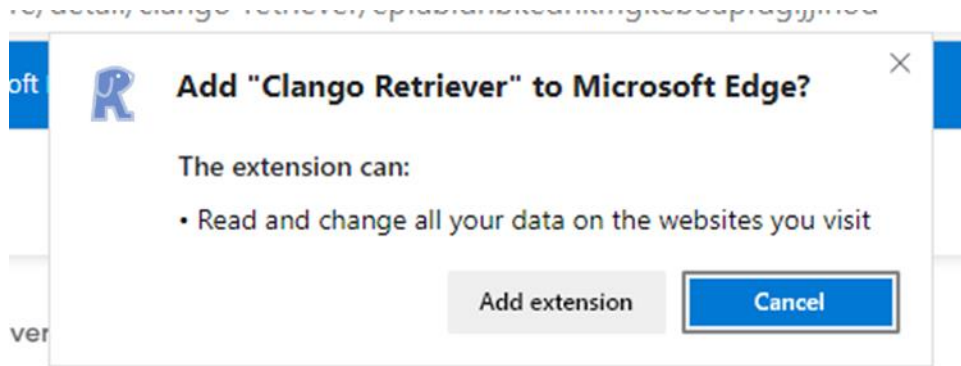


### 5.1.2 Edge

1. Navigate to <edge://extensions/>
2. In the menu on the left, enable **Allow extensions from other stores** and click **Allow** in the confirmation popup.

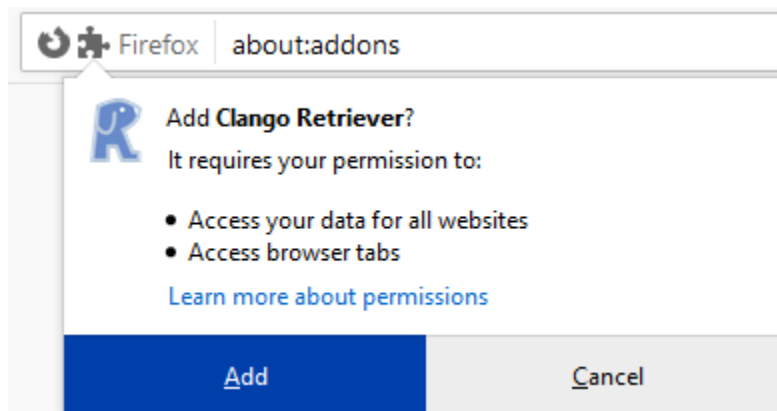


3. Navigate to <https://chrome.google.com/webstore/detail/clango-retriever/epfabidnbkednkmgkeboapfdgljjihod>.
4. Click **Add to Chrome**.
5. Click **Add extension** in the confirmation popup.



### 5.1.3 Firefox

1. In Firefox, open the Firefox menu button and click **Add-ons**.
2. From the settings (cog) dropdown menu, choose **Install Add-on From File**.
3. In the file dialog, browse to and open the XPI file provided.
4. Click **Add** in the confirmation popup.



## 5.2 Automatic Installation

### 5.2.1 Chrome

1. Download and install the Chrome AMDX files into your Group Policy.
  - a. Download Bundle 64 bit (GoogleChromeEnterpriseBundle64.zip) from <https://support.google.com/chrome/a/answer/7650032?hl=en>.
2. On one of your Domain Controllers, open **Group Policy Management Editor**.
3. Select the container where you want the policy to apply.
  - a. Edit the policy.
  - b. Find the "Extensions" container under: "Computer Configuration / Administrative Templates / Google / Google Chrome / Extensions".
  - c. If you want users to be able to disable or remove Retriever, skip to step h.
  - d. Enable **Configure the list of force-installed apps and extensions**.
  - e. Select the **Show** box under **Options**:

- f. In the **Value** field, add:  
epfabidnbkednkmgkeboapfdgljjihod;https://clients2.google.com/service/update2/crx
  - g. Skip to step k.
  - h. Enable **Extension management settings**.
  - i. Select the **Show** box under **Options**:
  - j. In the **Value** field, add:  

```
{"epfabidnbkednkmgkeboapfdgljjihod":{"installation_mode":"normal_installed","update_url":"https://clients2.google.com/service/update2/crx"}}
```
- Note: Make sure no returns are embedded within the string.**
- k. Choose **OK**.
4. It will install after the next Group Policy refresh and after Chrome has been closed and opened. To get it to install faster: at the user's workstation, run from the command prompt: gpupdate /force.
    - a. Wait a few minutes.
    - b. Close Chrome, then open it again, and it should be there.

### 5.2.2 Edge

1. Download and install Microsoft Edge Administrative Template.
  - a. Use the Get Policy Files link on the landing page at <https://www.microsoft.com/en-us/edge/business/download>.
2. On one of your Domain Controllers, open **Group Policy Management Editor**.
3. Select the container where you want the policy to apply.
  - a. Edit the policy.
  - b. Find the "Extensions" container under "Computer Configuration / Administrative Templates / Microsoft Edge / Extensions".
  - c. If you want users to be able to disable or remove Retriever, skip to step h.
  - d. Enable **Control which extensions are installed silently**.
  - e. Select the **Show** box under **Options**:
  - f. In the **Value** field, add:  
epfabidnbkednkmgkeboapfdgljjihod;https://clients2.google.com/service/update2/crx
  - g. Skip to step k.
  - h. Enable **Extension management settings**.
  - i. Select the **Show** box under **Options**:
  - j. In the **Value** field, add:  

```
{"epfabidnbkednkmgkeboapfdgljjihod":{"installation_mode":"normal_installed","update_url":"https://clients2.google.com/service/update2/crx"}}
```

**Note: Make sure no returns are embedded within the string.**

- k. Choose **OK**.
4. It will install after the next Group Policy refresh and after Edge has been closed and opened. To get it to install faster: at the user's workstation, run from the command prompt: `gpupdate /force`
  - a. Wait a few minutes.
  - b. Close Edge, then open it again, and it should be there.

### 5.2.3 Firefox

1. Download and install Firefox Administrative Template.
  - a. Located at <https://github.com/mozilla/policy-templates/releases>.
2. Put the Retriever XPI in a place where everyone has read access. For example, if the H drive is accessible to all target users, the path may look something like this:  
H:\Folder\FileName.xpi
3. On one of your Domain Controllers, open **Group Policy Management Editor**.
4. Select the container where you want the policy to apply.
  - a. Edit the policy.
  - b. Find the "Extensions" container under "Computer Configuration / Administrative Templates / Firefox / Extensions".
  - c. Enable **Control which extensions are installed silently**.
  - d. Select the **Show** box under **Options**:
  - e. Add the full network path to the XPI file (e.g., //path/to/file.xpi) to the **Value** field and choose **OK**.
  - f. If you want users to be able to disable or remove Retriever, skip to step 5.
  - g. Enable **Prevent extensions from being disabled or removed**.
  - h. Select the **Show** box under **Options**:
  - i. Add `retriever@clango.com` to the **Value** field and choose **OK**.
5. It will install after the next Group Policy refresh and after Firefox has been closed and opened. To get it to install faster: at the user's workstation, run from the command prompt: `gpupdate /force`
  - a. Wait a few minutes.
  - b. Close Firefox, then open it again, and it should be there.

## 6 Configure Retriever on User Workstations

Each user will have to manually configure Retriever after it is installed.

1. In the user's browser, click the Retriever icon.
2. You will see the **Settings** page, as follows:

**Retriever**

The extension must be configured.

CyberArk Server

Authentication Method

CyberArk Multi-Factor LDAP Windows Smart Card

Sync with PVWA logins  
 On  Off

Suggest usernames on log in forms  
 On  Off

Auto-populate forms when a single account is found  
 On  Off

Prompt to add account when new logon is detected  
 On  Off

Remember additional fields populated by the context menu  
 On  Off

Manage 0 Additional Login Fields

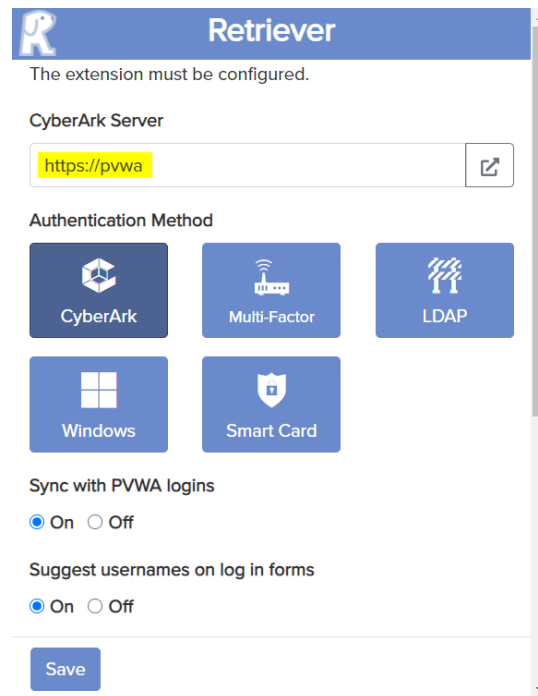
Manage 0 Ignored Sites

Open Account Suggest Popup Shortcut

ctrl + .

Save Cancel

3. In the CyberArk Server input, enter the URL for the PVWA server without the "PasswordVault" portion, e.g., <https://pvwa> if PVWA is accessible at <https://pvwa/PasswordVault>.



The screenshot shows the Retriever configuration interface. At the top, there is a blue header with the Retriever logo and the word "Retriever". Below the header, a message states "The extension must be configured." The "CyberArk Server" section contains a text input field with the URL "https://pvwa" and a copy icon. The "Authentication Method" section features five buttons: "CyberArk", "Multi-Factor", "LDAP", "Windows", and "Smart Card". Below this, there are two toggle switches: "Sync with PVWA logins" (set to On) and "Suggest usernames on log in forms" (set to On). A "Save" button is located at the bottom of the configuration area.

4. Select the authentication method that users usually use for logging into PVWA.
5. Click **Save**.
6. Confirm that the configuration is complete by logging in to Retriever using the same credentials a user would use with PVWA.