chrome enterprise

Virtual App and Desktop Launcher (V-Launcher)

Solution overview and deployment guide

Enterprise & Education

Table of contents

V-Launcher application scenarios

V-Launcher allows the secure and automatic launch of virtualized apps and desktops on managed Chrome OS devices.

- Launch shared virtualized desktops for kiosk devices
  V-Launcher is configured for an auto-launched Chrome OS managed guest session (MGS) or kiosk session. V-Launcher launches a dedicated virtualized desktop upon every session start and disconnect.

- Launch shared virtualized apps to enable Epic Fast User Switching (FUS) for shared clinical devices
  V-Launcher is configured as part of a Chrome OS Imprivata integration for a MGS. Upon every MGS launch and after every disconnect, V-Launcher launches the virtualized app with a device user account. The virtual session keeps running across users. User context is switched within the virtualized session.

How V-Launcher works

The solution consists of the following components:

- Chrome extension
- V-Launcher admin panel: web application
- Back-end components: web API and the database

Initial pairing of Chrome OS device and virtual resource

1. A factory new or power-washed Chrome OS device is enrolled in an organizational unit.
2. Upon the first launch of a managed guest session or user session, the V-Launcher extension force-installs.
3. The V-Launcher extension creates a new keypair (private key / public key) via the keystore.
4. The V-Launcher extension registers itself at the V-Launcher backend—transmitting hostname, serial number, and the public key of the freshly created keypair.
5. In the V-Launcher admin panel, you can look up the device's pending registration based on device hostname, location, or IP address.
6. To accept registration, you select an AD security group (controls access to VDI resources) and a specific VDI resource to auto-launch.
7. The V-Launcher back-end creates a new AD user for that device in the container specified during the installation.

Launch of virtual resource on device

1. V-Launcher extension requests Citrix launch config from V-Launcher backend based on the device-specific public key.
2. V-Launcher backend changes the associated device user's AD password, and requests the Citrix launch config file from Citrix for them via username and password.
3. V-Launcher backend transmits the Citrix launch config to the V-Launcher extension.
4. V-Launcher extension requests Citrix Workspace Chrome app via the Citrix SDK to launch the virtualized resource based on the Citrix launch config.
5. Citrix Workspace app launches the specified resource.
6. When the session gets disconnected, the V-Launcher extension relaunches the specified resource.

Active Directory objects that the V-Launcher backend communicates with

- AD security groups with virtualized resources assigned to them.
- AD security group for VDI admins—AD accounts must be members of this group to access the V-Launcher admin panel.
- AD container with VDI admins accounts—AD accounts must be placed in this container to access the V-Launcher admin panel.
- AD container for device accounts—The V-Launcher backend creates an account for each Chrome OS device during the registration process, so it is recommended to create a separate container for these accounts.

Set up V-Launcher

Before you begin

System requirements

1. Microsoft Windows Server 2008, 2012, 2016, or later, or Windows 10[1, 2]
2. Microsoft Active Directory Domain Services (AD DS)
3. Active Directory support configured to support SSL connection
4. Managed Chrome OS devices with Chrome Enterprise Upgrade
5. Citrix Virtual Apps and Desktops version 7.15 or later
6. PowerShell 5

Get parameters from AD domain controller

You can identify AD groups, containers, and users using their distinguished name (DN).

1. AD domain controller URL.
2. AD server SSL certificate thumbprint:
    1. Navigate to **Certification Authority**.
    2. Select the current server > **Issued Certificates**.
    3. Select the certificate of the domain controller.
    4. Click **Open** > **Details** > **Thumbprint**.
    5. Copy the value of the thumbprint and remove the spaces between the hexadecimal numbers, if space characters are present. See Microsoft documentation.
3. AD group for V-Launcher admins—Members of this group have permission to sign in to the V-Launcher admin panel.
4. AD container that contains V-Launcher admins—AD accounts attempting to sign in to the V-Launcher admin panel are looked up from this container.
5. AD container where new AD users will be created—Each user maps to a registered device.
6. AD container containing security groups that V-Launcher admins can choose from during device registration—A new AD user is created in one of the selected security groups as part of the registration. The security groups control access to VDI resources.

Get parameters from Citrix StoreFront

7. Citrix Store URL:
    1. Navigate to Citrix Studio.
    2. Click **Console Root** > **Citrix Store** > **Front Stores**.
    3. Select the store.
    4. Copy the value of the Store URL and save it for future use.
8. Enable the basic authentication feature on Citrix.

---

[1] To deploy the server to a Windows 10 machine, adjust the security settings by executing **Set-ExecutionPolicy Bypass -Scope Process** in the command line.
When the installation is completed, execute the **iisreset** command.

[2] All the Windows 10 machines must have remote PowerShell connection allowed by executing the **Enable-PSRemoting** command. On Windows Server 2012 and higher it's allowed by default.

Prepare a service account

1. Create a new AD user account. This account will be used as a service account for communication between the V-Launcher backend and the AD domain controller.
2. Grant the service account permissions to manage the container with security groups. See step 6 in the Parameters to retrieve from AD domain controller section.
    a. In Active Directory Users & Computers, right-click the container with security groups and click **Delegate Control**.
    b. On the Welcome to the Delegation of Control Wizard page, click **Next**.
    c. On the Users or Groups page, add the V-Launcher service account. Then click **Next**.
    d. On the Tasks to Delegate page, select **Delegate the following common tasks** and check the **Modify the membership of a group** task. Then click **Next**.
    e. On the Completing the Delegation of Control Wizard page, click **Finish**.
3. Grant the service account permissions to manage the container prepared for generated AD users accounts. See step 5 in the Parameters to retrieve from the AD domain controller section.
    a. In Active Directory Users & Computers, right-click the container prepared for generated AD users accounts and click **Delegate Control**.
    b. On the Welcome to the Delegation of Control Wizard page, click **Next**.
    c. On the Users or Groups page, add the V-Launcher service account. Then click **Next**.
    d. On the Tasks to Delegate page, select **Create a custom task to delegate**, and click **Next**.
    e. On the Active Directory Object Type page::
        i. Select **Only the following objects in the folder**.
        ii. Check the **User objects** in the objects types list.
        iii. Check the boxes next to **Create selected objects in this folder** and **Delete selected objects in this folder**.
        iv. Click **Next**.
    f. On the Permissions page, in the Permissions list, check the boxes next to **Read**, **Write**, **Read All Properties**, **Write All Properties**, and **Reset Password**. Then click **Next**.
    g. On the Completing the Delegation of Control Wizard page, click **Finish**.

Download V-Launcher

Download the installation kit for the back-end components.

V-Launcher Backend setup

Important: Before installing, make sure that you have backups of all target servers, especially database information.

Deploy the server

1. Unzip the build.
2. Start PowerShell 5 console as Administrator.
3. In PowerShell console, navigate to the unzipped folder, with setup.ps1 in the root.
4. Run the script with the command .\setup.ps1.
5. If the solution has already been installed on the device under the same username, you will be prompted to apply the previously selected parameters.
6. If the solution was not previously installed, your options are;
    - Single server installation on the current machine
    - Installation on multiple remote servers to provide redundancy
7. If a remote installation is applied, enter the hostnames or IP addresses of the following system components:
    - Primary database
    - Secondary database (one or many).
      Note: All PostgreSQL 13 data on secondary database servers will be overwritten with a copy from the primary database server.
    - Primary web API server with an admin panel
    - Secondary web API server with no admin panel
8. On request, enter admin credentials to connect to the requested remote machine.
9. On request, enter a password to create a PostgreSQL database.
10. Enter DN of the AD security group containing V-Launcher admin users (see step 3 of the Parameters to retrieve from AD domain controller section).
    Note: VDI admin users must be members of this group.
11. Enter the AD domain controller URL.
12. Enter the DN of the created service account. See the Prepare a service account section.
13. Enter the password of the created service account.
14. Enter DN of the AD container containing V-Launcher admin users. See step 4 of the Parameters to retrieve from AD domain controller section.
15. Enter DN of the AD container new users will be created in during device registration. See step 5 of the Parameters to retrieve from AD domain controller section.
16. Enter DN of the AD container containing security groups the V-Launcher administrators can choose from during device registration. See step 6 of the Parameters to retrieve from AD domain controller section.
17. Enter AD server SSL certificate thumbprint. See step 2 of the Parameters to retrieve from AD domain controller section.
    If this field is left empty, no certificate validation is performed.

18. Enter VDI AD user name prefix, for device accounts created by V-Launcher in AD. The default value is **User**. Maximum length is 10 characters.
19. Enter Citrix Store URL. See step 7 of the Parameters to retrieve from AD domain controller section.
20. Enter fully qualified domain name (FQDN) of the primary web API server.
21. (For remote installation) Enter FQDN of the secondary web API server on request.
22. Copy the displayed admin panel URL. Save for future use.
23. Copy the displayed extension policy. Save for future use. If the servers are not accessible for the Chrome OS devices by the URLs listed in the config, edit them manually after you copy it.

Note: This instruction applies to HTTPS networks. Otherwise, in steps 20 and 21 enter the hostname instead of a fully qualified domain name (FQDN).

Configure app and extension settings

Force-install extension on devices

1. Sign in to your Google Admin Console.
2. From the Admin console Home page, go to **Devices** > **Chrome**.
3. Click **Apps & extensions** > **Managed guest sessions**.
4. To deploy the extension to all devices, leave the top organizational unit selected. Otherwise, select a child organizational unit
5. Click **Add** > **Add Chrome app or extension by ID**.
6. Enter extension ID, **ealmhhchndokggijmjkoccoljcihbphe .**
7. Select **From custom URL .**
8. Enter **https://storage.googleapis.com/chromeos-mgmt-public-extension/v-launcher/v1-1/update_manifest.xml**
9. Under Installation policy, select **Force install**.
10. Click **Save**. If you configured a child organizational unit, you might be able to **Inherit** or **Override** a parent organizational unit's settings

Configure V-Launcher extension

1. Sign in to your Google Admin Console.
2. From the Admin console Home page, go to **Devices** > **Chrome** > **Apps & Extensions** > **Managed guest sessions**.
3. Click the Virtual App and Desktop Launcher (V-Launcher) extension.
4. Using the toggle, turn on **Allow access to keys**.
5. Configure the parameters. See example.
    - cmsServerUrls (required) - A set of URLs to the VDI CMS Servers that manage users and vdi configurations listed in steps 20 and 21 of Deploying the server section. Add /vdiCms as suffix.
    - citrixReceiverId (required) - Identifier of the Citrix Workspace Chrome OS app used to launch virtualized resources.
6. Click **Save**.

Example

```
{
  "cmsServerUrls": {
     "Value": [
            "https://v-launcher1.yourdomain.com/vdiCms",
            "https://v-launcher2.yourdomain.com/vdiCms"
        ]

  },
  "citrixReceiverId": {
    "Value": "haiffjcadagjlijoggckpgfnoeiflnem"
  }
}
```

Configure the Citrix app

To allow communication between the extension and the Citrix Workspace application, you need to allowlist the extension ID in the Citrix app policy.

1. Sign in to your Google Admin Console.
2. From the Admin console Home page, go to **Devices** > **Chrome** > **Apps & Extensions** > **Managed guest sessions**.
3. Click the Citrix Workspace app.
   Note: If not already done, make sure to configure the Citrix Workspace app for force installation.
4. Configure the parameters to allowlist the V-Launcher extension ID. See example below.

Example

```
{
    "settings": {
        "Value": {
            "settings_version": "1.0",
            "store_settings": {
                "externalApps": [
                    "ealmhhchndokggijmjkoccoljcihbphe"
                ]
            }
        }
    }
}
```

Pair Chrome OS devices and virtual resources

Launch extension on Chrome OS devices—Google Admin console

1. Turn on Chrome OS device
2. Manually launch a MGS. Or, wait until the MGS automatically launches.
3. Based on the previous configuration, the V-Launcher extension launches automatically and registers at the backend.

Assign virtual resources to Chrome OS devices—V-Launcher admin panel

1. Launch console.
   In the current version, the URL of the V-Launcher admin panel is the IP address of the server that the app is deployed to, appended with `/vdiadminpanel`.
   For example, https://v-launcher1.yourdomain.com/vdiadminpanel
2. Sign in using your AD account name in one of the following formats:
   - username@domain and AD password
   - domain\username and AD password
3. Switch to the **pending registration** tab.
4. Search for your target device using one of the following parameters:
   - Hostname
   - Location
   - IP address or IP range
5. Select the devices you want to assign a VDI resource to and click **Register**.
6. Assign a VDI resource:
   - Select a security group the devices belong to. The VDI resource list depends on the security group selected and configured on the Active Directory side.
   - Select a VDI resource from the dropdown list and complete the flow.
7. Based on the assignment, the V-Launcher backend creates an AD user for the selected device, thereby using the pre-configured user prefix.
8. Confirm assignment of virtual resource to device. Configured devices are shown on the **registered** tab

Note: You can edit assignments of virtual resources to devices at any time on the **registered** tab. The new configuration is applied during the next resource launch on the Chrome OS device.

Note: You can delete assignments of virtual resources to devices at any time on the **registered** tab.You can also delete the automatically created AD users. If the V-Launcher extension launches on a device with a deleted assignment, the device appears on the **pending registration** tab.

Troubleshoot

If you're experiencing issues with setting up V-Launcher, review these solutions to common issues.

Extension not starting on device

- Make sure that the extension is installed on the device.
- Make sure that the Citrix Workspace app is installed on the device.
- In the Google Admin console, make sure that the Citrix Workspace app has the extension id listed as an **externalApps** value.
- Make sure that the device can connect to the VDI extension backend and to the Citrix server.
- Open the V-Launcher admin panel and make sure that the device is displayed on the **Registered** tab and has a VDI resource assigned.

Extension not installed on device

In the Google Admin console, make sure that:

- The Chrome OS device or a specific user is displayed in the organizational unit.
- The organizational unit has the extension forced-installed on devices.

Device not showing up in V-Launcher admin panel

- Make sure that the extension is installed on the Chrome OS device;
- Make sure that the V-Launcher server is reachable from the Chrome OS device.

Extension consistently shows remote desktop disconnected notification

If the extension keeps showing the remote desktop disconnected notification after the device is power washed, make sure that the device is not present in the V-Launcher admin panel. If present, delete it.

Admin Panel unavailable when trying to access the V-Launcher admin panel using FQDN as a hostname

Use the machine name instead of FQDN.

V-Launcher admin panel requests containing FQDN fail with bad URI error

Open the admin panel config file located in **C:\inetpub\wwwroot\VdiAdminPanel\app.config.json** and remove the domain name from the cmsServerUrl value.

Extension requests fail with bad URI error

Check if the backend servers listed as the cmsServerUrls values in the chrome config in the Google Admin console are accessible from the chrome extension client devices.

Advanced Options

Export logs

You can export all table data as a .csv file. The provided data covers the whole period of the system activity.

Disable auto-reconnect

By default, all devices are set to reconnect automatically when they get disconnected from the VDI resource. You can turn off the auto-reconnect by selecting the dedicated checkbox in the Register or Edit wizard in the V-Launcher admin panel. With auto-reconnect turned off, the extension user will get a sticky notification on the VDI resource being disconnected. Users can initiate reconnection by clicking **Reconnect** on the notification. Or, they can try restarting the device.