chrome enterprise

# Virtual App and Desktop Launcher (V-Launcher)

Solution overview and deployment guide

Enterprise & Education

# Table of contents

**V-Launcher**

**Installation Guide**

**V-Launcher application scenarios**

**How V-Launcher works**

- Initial Pairing of V-Launcher
- VDI Allocation and ChromeOS Device Registration
- Launch of a virtual resource on the device
- Active Directory Components Used by V-Launcher

**Set up V-Launcher**

- Before you begin: System Requirements
- Prerequisites for V-Launcher Setup
  - Prepare a service account
- Steps within the Installation Script

**Troubleshoot**

- Extension not starting on device
- Extension not installed on device
- Device not showing up in V-Launcher admin panel
- Make sure that the Chromebook is within the same network.
- The extension consistently shows a remote desktop disconnected notification

**Recovery Flow for V-Launcher**

- Encrypted Recovery File (.vlnrc)
- How the Recovery Process Works

# V-Launcher

## Installation Guide

**V-Launcher** is a virtualized application and desktop launcher designed for managed Chrome OS devices. It provides a smooth and secure experience for launching and managing virtual applications and desktops while ensuring streamlined device registration and resource assignment.

The solution consists of the following components:

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

## 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**
  V-Launcher is configured for an auto-launched Chrome OS managed guest session (MGS) or a user-signed-in session. V-Launcher launches a dedicated virtualized desktop upon every session start and disconnects.

- **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

## Initial Pairing of V-Launcher

1. Ensure the ChromeOS device is factory-new or power-washed and enrolled in an organizational unit.
2. Upon the first launch of a **user session** or **managed guest session**, the **V-Launcher extension** will be **auto-installed**.
3. The V-Launcher extension **automatically enrolls** with the **V-Launcher backend service**. transmitting hostname, serial number and IP address,
4. In the **V-Launcher admin studio**, you can look up the device's **pending registration** based on:
    - Device hostname
    - Location
    - IP address

## VDI Allocation and ChromeOS Device Registration

1. Navigate to the **V-Launcher admin studio.**
    - URL: http://localhost/vlauncher/admin
2. Go to the **Pending Devices** section.
    - View the list of **pending ChromeOS devices.**
3. Select the devices from the table and click the "**+**" button (top-right corner). The V-Launcher back-end creates a new AD user for that device in the container specified during the installation.
4. Assign the following:
    - **Active Directory Group**
    - **VDI resources** from the **VDI Resources section**
5. **Enable Auto-Launch** for required VDIs from the right-side table and register the device.

## Launch of a virtual resource on the device

1. The **V-Launcher extension** requests **Citrix to launch ICA data** from the **V-Launcher backend** using the **auto-generated device ID.**
2. The **V-Launcher backend** sends **Active Directory credentials** to the **Citrix Storefront server** to retrieve ICA data. 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. The **ICA data** is transmitted to the **V-Launcher extension.**
4. The **V-Launcher extension** requests the **Citrix Workspace Chrome app** (via the Citrix SDK) to launch the virtualized resource.  based on the Citrix launch config.
5. The **Citrix Workspace app** launches the specified resources through the extension to the user's Chromebook.
6. When the session gets disconnected, the V-Launcher extension relaunches the specified resource.

**Note:** You can edit assignments of virtual resources to devices at any time on the registered tab. The new configuration will be notified of the changes in real time via the extension or will be 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. If the V-Launcher extension launches on a device with a deleted assignment, the device appears on the pending registration tab.

## Active Directory Components Used by V-Launcher

- Active Directory Organizational Units (OUs)
    - The V-Launcher application requires three distinct Sub OUs under the main OU:
        - **ChromeOS Devices Container** – Stores Active Directory accounts for ChromeOS devices. 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.
        - **Administrator Container** – Contains security groups for administrators and admin users, who will be placed within this container.
        - **Citrix VDI Resources Container** – Holds security groups assigned to Citrix VDI resources.
- Active Directory Security Group for Administrators under the Administrator Container
    - **Administrator accounts** must be members of this group.
- Active Directory Certificate Service

# Set up V-Launcher

## Before you begin: System Requirements

- Windows Server 2012, 2016, or later
- Microsoft Active Directory Domain Services (AD DS)
- Active Directory Certificate Services (DC Server)
    - Certification Authority
- DNS Server (DC Server)
    - Add the DC server SSL certificate to the trusted root certificate store in the V-Launcher backend deployment server
- Web Server (IIS) on V-Launcher Backend Server
    - Common HTTP Features:
        - Default Document, Directory Browsing, HTTP Errors, Static Content
    - Health & Diagnostics:
        - HTTP Logging
    - Performance:
        - Static Content Compression
    - Security:
        - Request Filtering
    - Application Development:
        - Application Initialization, WebSocket Protocol
- ChromeOS devices with Chrome Enterprise Upgrade
- Citrix Virtual Apps & Desktops 7.15 or later
- PowerShell 5

## Prerequisites for V-Launcher Setup

1. Active Directory Main Organizational Unit (OU)
2. Active Directory Sub-Organizational Units (Sub OUs)
    a. ChromeOS Devices Container – Stores AD accounts for ChromeOS devices.
    Format: OU=DemoDevices,DC=citrix,DC=lab
    b. Administrator Container – Contains security groups for administrators.
    Format: OU=DemoAdmins,DC=citrix,DC=lab
    c. Citrix VDI Resources Container – Holds security groups assigned to Citrix VDI resources.
    Format: OU=DemoVDI,DC=citrix,DC=lab
3. Microsoft Active Directory Domain Services (AD DS)
    a. Create an AD security group for administrator access under the above-created Administrator Container (In step 1).
    Preferred format: CN=DemoAdmin_users,OU=DemoUsers,DC=citrix,DC=lab
    b. Ensure all administrator accounts are members of this group. (These administrator accounts will be used to log in for the V-Launcher Admin Studio)
4. VDA Group
    a. Active Directory Certificate Services

        - Must be installed on the Domain Server.
    b. Domain Server Certificate
        - Must be placed under "Trusted Root CAs" on the client machine.
5. Create the Service Account User and Delegate Control for that user.

## Prepare a service account

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.

- Grant the service account permissions to manage the container with security groups.
    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.

- Grant the service account permissions to manage the container prepared for the generated AD user accounts.
    a. In Active Directory Users & Computers, right-click the container prepared for generated AD user 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 object 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.

## Steps within the Installation Script

1. **Unzip** the downloaded installation kit: V-Launcher Installation Kit
2. **Run the setup script on the Client machine:**
    a. Right-click on the setup file and Run with PowerShell.
    b. Open PowerShell and run **./setup.ps1** directly.
    c. Alternatively, navigate to the script directory and execute **./setup.ps1** from there.
    (The installation script will automatically check the IIS availability and will automatically install the IIS and required modules.)
3. Provide PostgreSQL Credentials:
    a. Enter a **username** and **password** as requested by the PostgreSQL installation script.
    (The installation script will automatically verify the availability and install it if it is not already present. Otherwise, it will access the existing PostgreSQL instance.)
    The system is allowing PostgreSQL to connect through the firewall port 5432.
4. Users need to add the following details, which are manually configured in the Domain Server:
    a. Enter The Devices Container Distinguished Name
    b. Enter The VDI Container Distinguished Name
    c. Enter The Service Account Distinguished Name
    d. Enter The Service Account User Principal Name
    e. Enter The Service Account Password
    f. Enter The Admins Container Distinguished Name
    g. Enter The Admin Security Group
    h. Enter The LDAPS Address
5. Next, authenticate with PostgreSQL by giving the PostgreSQL username and password once the AD configuration is complete.
6. Provide a database name for V-Launcher.
7. Enter the Citrix StoreFront URL. Get the URL from Citrix StoreFront:
    1. **Log in to the Citrix StoreFront server.**
    2. Open the **Citrix StoreFront Management Console**.
    3. In the left-hand pane, click "**Stores**".
    4. Click the name of your store.
    5. Under the detail tab, you will find the **StoreFront URL**.
        - https://storefront.yourcompany.com/Citrix/StoreWeb/
    6. Enable the basic authentication feature on Citrix.

(The database structures required for the V-Launcher solution will be migrated.)

8. Force install the V-Launcher extension and the Citrix Workspace App on Chrome devices
(Applies to both Managed Guest Sessions and User Sign-In Sessions)
    a. Sign in to the Google Admin Console: admin.google.com
    b. Navigate to:
        i. Devices > Chrome > Apps & extensions > Managed guest sessions (for MGS)
        ii. Devices > Chrome > Apps & extensions > Users & browsers (for signed-in users)
    c. Select the organizational unit (OU) where you want to apply the policy
        i. Top-level OU for all devices/users
        ii. Child OU for specific groups
    d. Click Add > Add Chrome app or extension by ID

e. Enter the:
    i. V-Launcher Extension ID: ocngoaellimggbdhenclkhmfggoljecc
    ii. Citrix Workspace App ID: haiffjcadagjlijoggckpgfnoeiflnem
f. Choose From the Chrome Web Store
g. Under the Installation policy, select Force install
h. Click Save

9. The JSON Values needed to be set within the V-Launcher Extension and Citrix Workspace App in the Google Admin Console, under Apps & Extensions, for the Users & Browser section.

The JSON to add in the Google Admin Console under the V-Launcher extension (Extension ID: ocngoaellimggbdhenclkhmfggoljecc)

```
{
    "studioURL": {
      "Value": "http://<YOUR_SERVER_FQDN>/vlauncher/api/extension"
    },
    "citrixAppID": {
      "Value": "haiffjcadagjlijoggckpgfnoeiflnem"
    }
}
```

The JSON to add in the Google Admin Console under the Citrix Workspace App (App ID: haiffjcadagjlijoggckpgfnoeiflnem)

```
{
    "settings": {
      "Value": {
        "settings_version": "1.0",
        "store_settings": {
          "externalApps": [
            "ocngoaellimggbdhenclkhmfggoljecc"
          ]
        },
        "engine_settings": {
          "vc_channel": {
            "CTXTUI": false
          }
        }
      }
    }
}
```

10. Enter the password for the encrypted recovery file.
11. Access the V-Launcher Admin Studio using the provided URL: http://localhost/vlauncher/admin

```
{
    "studioURL": {
      "Value": "http://<YOUR_SERVER_FQDN>/vlauncher/api/extension"
    },
    "citrixAppID": {
      "Value": "haiffjcadagjlijoggckpgfnoeiflnem"
    }
}
```

# 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 latest version of the extension is installed on the device.
- Make sure that the Citrix Workspace app is installed on the device.
- 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.

## Make sure that the Chromebook is within the same network.

## The extension consistently shows a 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.

# Recovery Flow for V-Launcher

If the V-Launcher application or its configuration becomes corrupted, deleted, or the IIS Application Pool is reset, administrators can use the recovery process described below to securely restore operational credentials and settings.

## Encrypted Recovery File (.vlnrc)

During the initial installation, a .vlnrc file is generated and encrypted using AES-256. The administrator is prompted to set a secure password, which is used (via SHA-256 hashing) to derive the encryption key. This file includes the critical application settings and Active Directory credentials used by V-Launcher.

**Important**: This file is the only backup of credentials and configuration. Recovery requires both the **.vlnrc** file and the password that was set during the installation process.

## How the Recovery Process Works

If recovery is needed:

1. **Locate the .vlnrc file** that was saved after the initial installation.
2. **Run the V-Launcher recovery script** on the backend server.
3. **Enter the original recovery password** when prompted.
4. The script will decrypt the **.vlnrc** file using the password.
    a. Users will have the ability to use the same decrypted configurations or modify the existing configurations.
5. The application automatically restarts using the restored configuration.
6. Once the recovery completes, a new .vlnrc file is generated with updated credentials and a **new recovery password** (Should enter new password at the end of the recovery script). This password must be saved and used for any future recovery operations.