This documentation covers the overview, setup, use, and background operations of the Login Enterprise Launcher Manager.

Launcher Manager: Overview

The Login Enterprise Launcher Manager (LM) is a centralized orchestration appliance designed to automate the lifecycle of Login Enterprise Launchers. It streamlines the process of commissioning, starting, stopping, and decommissioning launchers across your environment, ensuring that your performance testing infrastructure is always ready for execution.

Launcher Manager: Architecture

Launcher Manager (LM) is a customer-deployable appliance used to centrally manage and automate Login Enterprise Launchers. In the MVP, LM focuses on keeping launcher inventory aligned with Login Enterprise and providing reliable start/stop and lifecycle actions (commission/decommission) through an automation layer. Below will provide an overview of the components and protocols of the Launcher Manager and how they are being used.

Launcher Manager appliance:

The appliance is provided as an OVA file. The appliance hosts the LM web UI/API as well as the automation services that execute jobs and keep data in sync. Users interact with the LM UI to view launchers, map credentials, apply policies, and trigger actions.

Login Enterprise appliance:

Login Enterprise remains the source of truth for launchers and launcher group membership. Launcher Manager integrates with the Login Enterprise Public API to read launcher and group data and reflect that state inside LM.

Launchers:

Launchers are the Windows machines (or VMs) where the Login Enterprise Launcher software runs. Launcher Manager connects to these machines directly to perform configuration actions and to start/stop launcher activity.

HTTPS (TCP 443):

HTTPS is used for two primary flows. First, Launcher Manager communicates with the Login Enterprise Public API over 443 to synchronize launcher inventory and launcher group membership and to obtain any related data needed for orchestration. Second, users access the Launcher Manager web UI/API over 443.

SSH (TCP 22):

SSH is used as the primary remote execution channel from Launcher Manager to each launcher. The Rundeck jobs use SSH to run PowerShell commands on the launcher, validate connectivity, perform commissioning/decommissioning tasks, stop processes such as the LoginEnterprise.Launcher.UI, and perform session cleanup steps.

RDP (TCP 3389):

RDP is used for workflows that require an interactive user session context. In this iteration of the Launcher Manager, this is primarily associated with the “Start” behavior where the launcher UI is expected to be running in a real session. LM establishes or leverages an RDP session to ensure the launcher starts reliably and behaves consistently.

Session handling (tscon and logoff)

The automation workflows also manage Windows session state. tscon may be used to transfer an RDP session to the console (or otherwise normalize session behavior) so the launcher can continue running as intended when the initiating RDP client disconnects. During “Stop,” the scripts enumerate sessions for the service account and log off relevant console/RDP/disconnected sessions to prevent orphaned sessions and ensure the launcher is fully stopped.

Below will outline the connectivity and firewall requirements for Launcher Manager.

Between Launcher Manager and Login Enterprise:

Launcher Manager must be able to reach the Login Enterprise appliance’s Public API over HTTPS (TCP 443). This is required for continuous synchronization of launcher inventory and launcher group membership, and to keep LM’s UI and automation decisions aligned with what Login Enterprise reports.

Between Launcher Manager and each Launcher:

Launcher Manager must be able to reach each launcher over SSH (TCP 22) to execute remote commands and perform management actions. Launcher Manager must also be able to reach each launcher over RDP (TCP 3389) for interactive start/session workflows.

Name resolution (DNS):

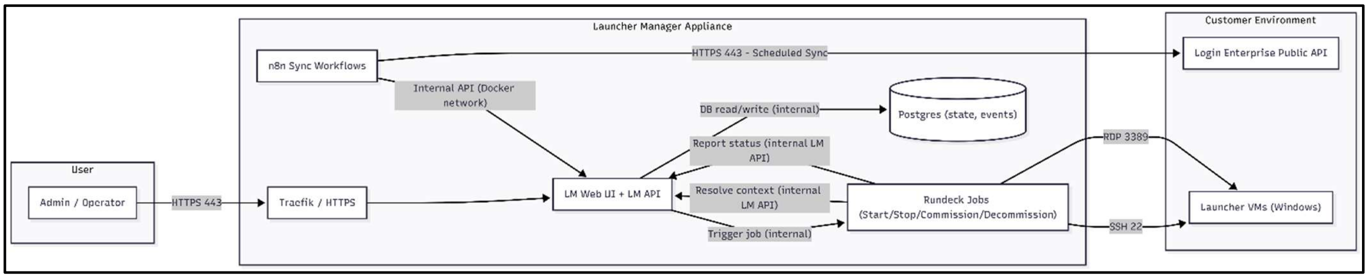
Reliable DNS/name resolution is required so Launcher Manager can resolve the Login Enterprise hostname and each launcher hostname (and vice versa where applicable). This prevents automation failures caused by hostname resolution issues and simplifies operations.

Internal workflow summary (what happens during an action):

When a user initiates an action (for example, Stop), the LM UI/API triggers a Rundeck job. The job calls the LM API to resolve the target launcher connection context (host, port, username, and secret). Rundeck then uses SSH to run the required PowerShell steps on the launcher (stop the launcher UI process, enumerate sessions, log off sessions as needed). Finally, the job posts status/results back to LM so the UI reflects the completed state and an event record is stored.

Port summary (MVP)

TCP 443: User to Launcher Manager (UI/API), Launcher Manager to Login Enterprise Public API
TCP 22: Launcher Manager to Launchers (SSH remote execution)
TCP 3389: Launcher Manager to Launchers (RDP interactive session workflows)
TCP/UDP 53: DNS resolution for Login Enterprise and launcher hostnames


Launcher Manager Appliance
n8n Sync Workflows
HTTPS 443 - Scheduled Sync
Customer Environment
Login Enterprise Public API
Internal API (Docker network)
DB read/write (internal)
Postgres (state, events)
RDP 3389
Report status (internal LM API)
User
Admin / Operator
HTTPS 443
Traefik / HTTPS
LM Web UI + LM API
Resolve context (internal LM API)
Rundeck Jobs (Start/Stop/Commission/Decommission)
Trigger job (internal)
SSH 22
Launcher VMs (Windows)

Phase 1: Environment Preparation

Before deploying the appliance, you must prepare your network and launcher machines.

1. Service Account Requirements

Create a dedicated Active Directory Service Account (e.g., svc_launcher_mgr). This service account will need Local Admin rights on the launcher machines as well as being allowed logon through Remote Desktop Services

2. DNS Configuration

The Launcher Manager must be resolvable by your Launchers for automations and events to function.

3. Launcher VM Configuration (OpenSSH)

Every Launcher must have the OpenSSH Server installed.

PowerShell Setup Script:

```
# 1. Install OpenSSH Server
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

# 2. Set Service to Automatic and Start it
Set-Service -Name sshd -StartupType Automatic
Start-Service sshd

# 3. Configure Firewall
Set-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -Profile Any
Enable-NetFirewallRule -DisplayName "OpenSSH SSH Server (sshd)"

# 4. Modify config to allow password authentication
$sshdConfig = "C:\ProgramData\ssh\sshd_config"
(Get-Content $sshdConfig) -replace "#PasswordAuthentication yes",
"PasswordAuthentication yes" | Set-Content $sshdConfig
Restart-Service sshd
```

Phase 2: Appliance Deployment

1. **Import OVA**: Import the Launcher_Manager.ova file into your hypervisor
2. **Provision Resources:** Configure the virtual machine with the following recommended specifications:
    - vCPU: 4
    - Memory: 8 GB RAM
    - Disk: 50 GB

3. **First Boot**: Power on the VM to trigger the Setup Wizard
4. **Configuration**: Follow prompts to set Network, Hostname, Login Enterprise credentials, and API Token
5. **Completion**: Once finished, navigate to the Web Interface URL displayed and login with the basic auth Login Enterprise credentials entered during the setup wizard

Phase 3: Background Automations

The Launcher Manager maintains synchronization with your Login Enterprise appliance through two background n8n workflows. These ensure the LM dashboard is always current.

- **Launcher Sync Workflow**: Queries the Login Enterprise API to update the status and registration details of all launchers every 60 seconds
- **Launcher Group Sync Workflow**: Synchronizes group memberships from Login Enterprise every 60 seconds

Note: For all Launcher Group management, Login Enterprise remains the absolute source of truth. Any changes to group names or memberships must be made within the Login Enterprise interface as the Launcher Manager appliance will automatically ingest these changes during the next sync cycle

Phase 4: Launcher Management Web App

The Launcher Manager web application is divided into four primary sections, each serving a critical role in the orchestration of your environment. All management actions are powered by Rundeck automation actions running on the appliance.

1. Launchers

The Launchers tab is your central command center for machine lifecycle management. It displays all launchers synced from Login Enterprise, including their online status, IP addresses, and current configuration.

NOTE: Launcher Manager does NOT perform discovery of existing or new launchers in your Login Enterprise environment. If the launcher is not manually registered or imported into Launcher Manager, then Launcher Manager will not know about the launcher.

2. Credentials

The Credentials tab stores the identities used to access your launcher fleet. Credentials are securely stored and mapped to specific launchers to ensure the appliance has the necessary permissions for software installation and interactive sessions.

3. **Policies**

The Policies tab defines the operational "rules" for your launchers. Policies include settings for specific startup arguments for things like the launcher application and Autologin preferences. Assigning a policy to a group of launchers ensures they all behave identically during testing cycles.

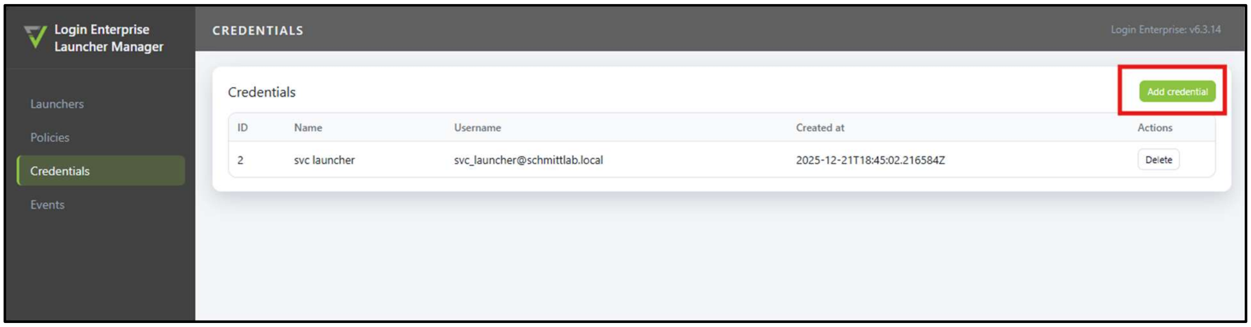
4. **Events**

The Events tab provides a real-time and historical audit trail of all automated tasks. Every action (Commission, Start, Stop) is logged with a unique Run ID. You can view the specific output of Rundeck actions to troubleshoot connectivity issues or installation errors

Phase 5: Using the Launcher Manager

Follow the steps below to use the web application and to begin leveraging the Launcher Manager to manage launchers in your Login Enterprise environment.

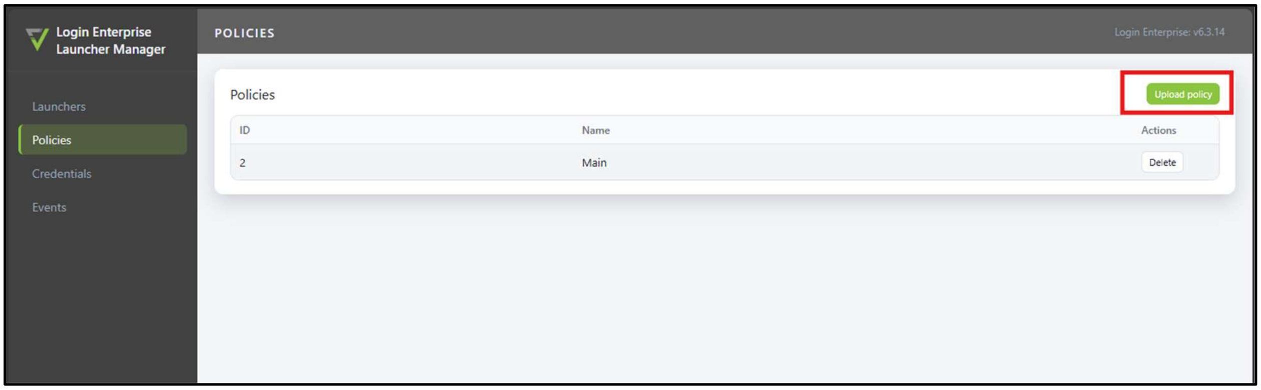
1. Navigate to the **Credentials** page > Select **Add credential**



ID	Name	Username	Created at	Actions
2	svc launcher	svc_launcher@schmittlab.local	2025-12-21T18:45:02.216584Z	Delete

2. Enter the username (svc_launcher@loginvsi.com) and password of the service account that will be used to SSH and perform tasks on the launchers

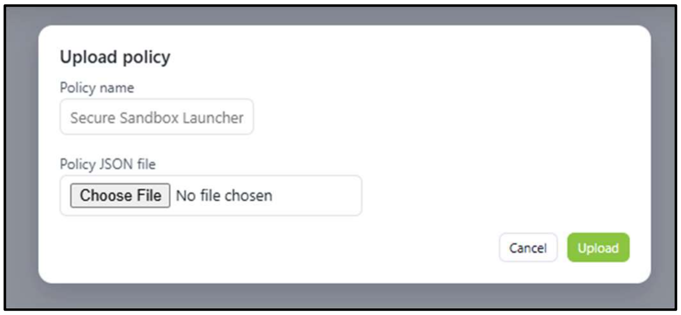
3. Navigate to **Policies** > Select **Upload Policy**



Policies

ID	Name	Actions
2	Main	Delete

4. Provide the name of the policy to upload and select the JSON configuration file that will be used by the management actions on what actions to perform on the launchers



Upload policy

Policy name: Secure Sandbox Launcher

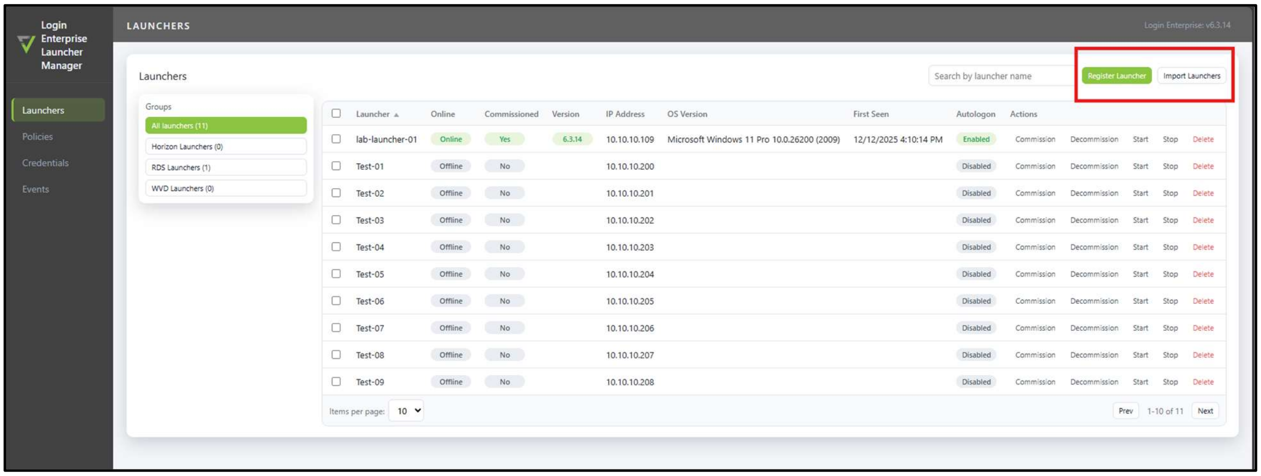
Policy JSON file: No file chosen

Use the JSON template located at {Insert GitHub link HERE} to upload and create a policy from. This can be adjusted as needed for the actions that are performed by the Launcher Manager management actions. The JSON policy will enable the following actions to be performed if set to true:

- **launcher: true**
  - Installs the Login Enterprise Launcher software on the target launcher machine
- **uwc: true**
  - Installs the Universal Web Connector (UWC) on the launcher machine
- **autologon: true**
  - Enables Windows autologon on the launcher machine and creates a Login Enterprise Launcher shortcut in the Startup folder so the launcher application starts automatically after login
- **uwcPullScripts: true**
  - Enables automatic retrieval of existing Universal Web Connector (UWC) scripts from the Login Enterprise appliance during the Commission action.

When **uwcPullScripts** is enabled, the Login Enterprise appliance must contain a **/loginvsi/content/** directory populated with a zipped archive of UWC scripts. During the commissioning process, the Launcher Manager will pull this archive from the appliance, extract the scripts, and ensure that the **ProgramData\LoginVSI\UWC\Scripts** directory exists on the launcher machine, creating it if necessary

5. Navigate to **Launchers** > Select either **Register Launcher** or **Import Launchers**

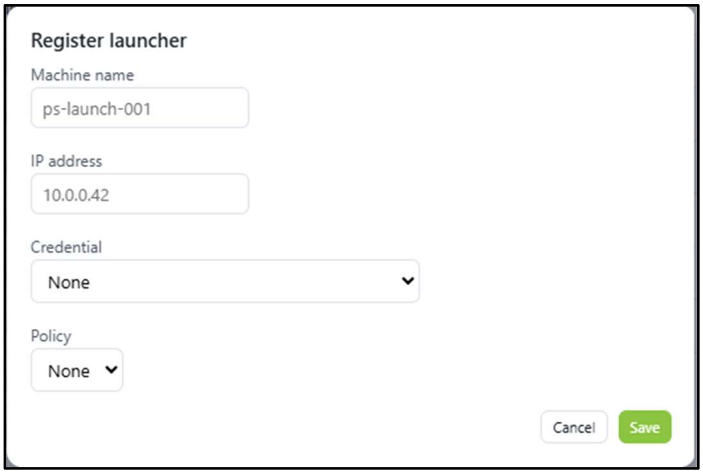


☐	Launcher ▲	Online	Commissioned	Version	IP Address	OS Version	First Seen	Autologon	Actions
☐	lab-launcher-01	Online	Yes	6.3.14	10.10.10.109	Microsoft Windows 11 Pro 10.0.26200 (2009)	12/12/2025 4:10:14 PM	Enabled	Commission Decommission Start Stop Delete
☐	Test-01	Offline	No		10.10.10.200			Disabled	Commission Decommission Start Stop Delete
☐	Test-02	Offline	No		10.10.10.201			Disabled	Commission Decommission Start Stop Delete
☐	Test-03	Offline	No		10.10.10.202			Disabled	Commission Decommission Start Stop Delete
☐	Test-04	Offline	No		10.10.10.203			Disabled	Commission Decommission Start Stop Delete
☐	Test-05	Offline	No		10.10.10.204			Disabled	Commission Decommission Start Stop Delete
☐	Test-06	Offline	No		10.10.10.205			Disabled	Commission Decommission Start Stop Delete
☐	Test-07	Offline	No		10.10.10.206			Disabled	Commission Decommission Start Stop Delete
☐	Test-08	Offline	No		10.10.10.207			Disabled	Commission Decommission Start Stop Delete
☐	Test-09	Offline	No		10.10.10.208			Disabled	Commission Decommission Start Stop Delete

Register Launcher

Allows you to manually register a single launcher into the Launcher Manager inventory. Provide the machine name and IP address, then select the credential and managed policy that should be associated with this launcher. Credentials and policies must already exist and be created in the previous steps.

Once saved, the launcher will appear in the inventory and can immediately be commissioned, decommissioned, or managed using Launcher Manager automation actions.



Register launcher

Machine name: ps-launch-001

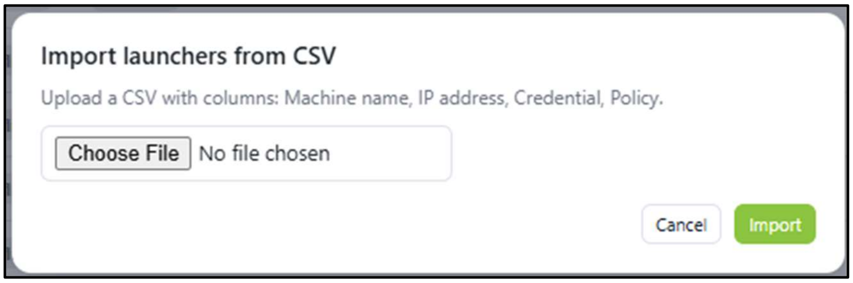
IP address: 10.0.0.42

Credential: None

Policy: None

Import Launchers

Allows you to bulk import multiple launchers using a CSV file. A sample CSV file can be found at {Insert GitHub link HERE}. Each row must include the machine name, IP address, credential ID, and policy ID to associate with the launcher. Credential and policy IDs can be obtained from the Credentials and Policies pages. Once imported, the launchers will be registered in Login Enterprise and available for management actions.



Import launchers from CSV

Upload a CSV with columns: Machine name, IP address, Credential, Policy.

No file chosen

Available Management Actions:

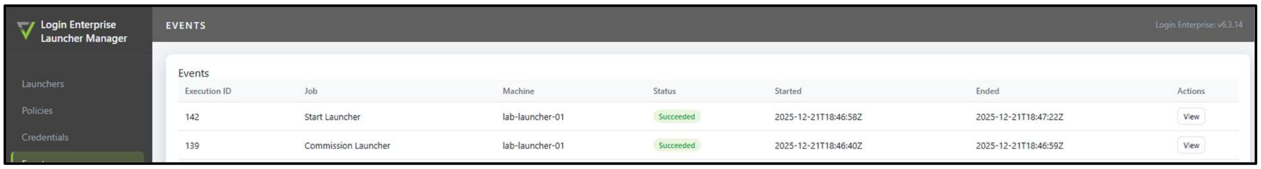
- **Commission:** Performs the initial setup of the launcher. This action uses SSH to transfer and install the Launcher software (MSI), Universal Web Connector (UWC), and necessary configurations. This step also enables Autologin if it is defined within the assigned policy
- **Decommission:** Gracefully removes the launcher software and registration from the target machine
- **Start:** Leverages xfreerdp to initiate an RDP session to the machine and start the Login Enterprise Launcher software
- **Stop:** Remotely terminates the launcher process on the host operating system

NOTE: If a launcher already exists and is actively running in the Login Enterprise environment, any manual registration or creation of that launcher in Launcher Manager must use the exact same machine name as shown in Login Enterprise.

Matching the machine name is required for the n8n workflows to function correctly, as these workflows rely on the machine name to synchronize launcher state between the Login Enterprise appliance and the Launcher Manager appliance.

If you are commissioning a machine that is not currently registered or running as a launcher in Login Enterprise, the machine name entered in Launcher Manager will be used to create and register the launcher in Login Enterprise during the Commission management action. In this case, the name provided in Launcher Manager becomes the authoritative launcher name that appears in Login Enterprise.

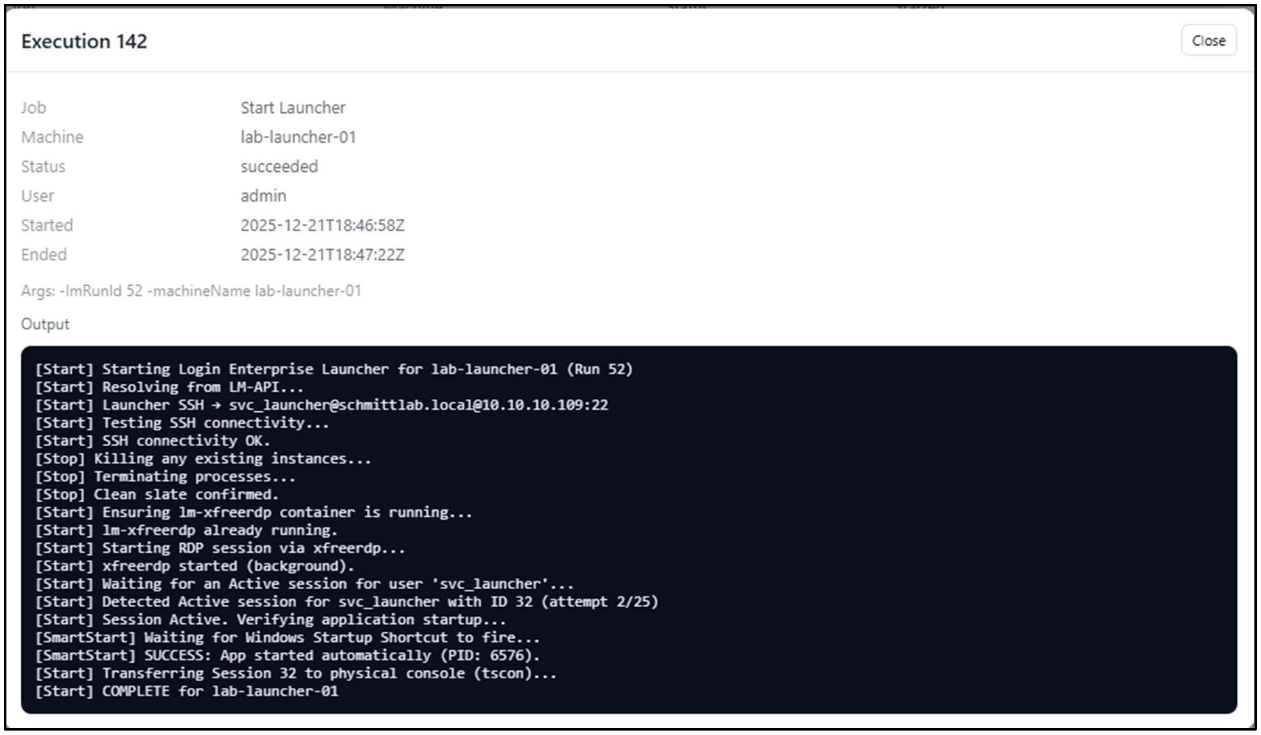
6. Once Launcher Manager actions have been run (Start, Stop, etc.), navigate to the Events tab to view an audit log of all automated action runs.



Events

Execution ID	Job	Machine	Status	Started	Ended	Actions
142	Start Launcher	lab-launcher-01	Succeeded	2025-12-21T18:46:58Z	2025-12-21T18:47:22Z	View
139	Commission Launcher	lab-launcher-01	Succeeded	2025-12-21T18:46:40Z	2025-12-21T18:46:59Z	View

Select **View** on an individual action record to see detailed steps of what was performed on the launcher machine.



Execution 142

Job	Start Launcher
Machine	lab-launcher-01
Status	succeeded
User	admin
Started	2025-12-21T18:46:58Z
Ended	2025-12-21T18:47:22Z

Args: -lmRunId 52 -machineName lab-launcher-01

Output

```
[Start] Starting Login Enterprise Launcher for lab-launcher-01 (Run 52)
[Start] Resolving from LM-API...
[Start] Launcher SSH → svc_launcher@schmittlab.local@10.10.10.109:22
[Start] Testing SSH connectivity...
[Start] SSH connectivity OK.
[Stop] Killing any existing instances...
[Stop] Terminating processes...
[Stop] Clean slate confirmed.
[Start] Ensuring lm-xfreerdp container is running...
[Start] lm-xfreerdp already running.
[Start] Starting RDP session via xfreerdp...
[Start] xfreerdp started (background).
[Start] Waiting for an Active session for user 'svc_launcher'...
[Start] Detected Active session for svc_launcher with ID 32 (attempt 2/25)
[Start] Session Active. Verifying application startup...
[SmartStart] Waiting for Windows Startup Shortcut to fire...
[SmartStart] SUCCESS: App started automatically (PID: 6576).
[Start] Transferring Session 32 to physical console (tscon)...
[Start] COMPLETE for lab-launcher-01
```