Recast

Temporarily Elevate User Privileges to Run Actions

Last Modified on 2026-07-21

As an Application Workspace administrator, you can temporarily grant a non-administrator user (meaning a user who is not a member of the local Administrators group) elevated admin privileges that allow them to run specific Application Workspace actions as the current logged-on user. This feature is suited to scenarios where there's a requirement to preserve the logged-on user's identity, such as when installing per-user application or setting up user-context firewall rules, while also allowing administrative operations to run.

> **Security Considerations**
>
> To maintain security while allowing elevated access, this feature includes a number of constraints:
> - Once the action completes, the user's elevated permissions do not persist, regardless of whether the action succeeds or fails.
> - The feature limits elevated access to the action being run. Privileges do not extend to other processes or sessions.
> - The user does not become a member of the local Administrators group at any point.
> - The elevation mechanism limits execution to approved/allowed programs and restricts token privileges to what is required.
>
> At the same time, administrators must accept inherent risks associated with privilege elevation:
> - Actions with scripting, such as script-based installers or a Start Process action with script arguments, can be exploited through malicious scripts executed with elevated rights.
> - Open File Explorer extensions may allow a user to launch other applications as an Administrator (for example, opening PowerShell from a context menu with elevated rights).

Enable Process Elevation

An Application Workspace administrator must enable the Process Elevation option, which is disabled and hidden by default.

To enable process elevation:

1. Open Application Workspace in its embedded browser via the Smart Icon or the Application Workspace portal.

2. Open the developer console:
   - For an embedded browser (WebWindow) – Click the `F12` key or use the application's developer tools shortcut
   - For a browser-based portal – Click the `F12` key and navigate to the **Console** tab

3. In the browser console, enable Developer Mode by entering the `DEBUG=1` command and clicking the Enter key.

4. In the Application Workspace interface, navigate to **Agent Settings**.

5. Under **Process Elevation**, enable **Use enhanced mode**. The feature becomes active for the current agent session.

> The `DEBUG=1` setting, as well as the feature's visibility in the interface, are limited to a browser session. If the browser is closed or restarted, you'll need to reactivate Developer Mode to access the **User Privilege Elevation** option.
>
> The enabled/disabled state of the feature itself will persist in the Agent configuration.

Recast

Configure an Action to Run Within the Elevated User Context

Once you enable process elevation, 'Elevated user' appears as a new Context option in the Action editor.

Supported Actions

You can choose 'Elevated user' as a context for the following actions:

- Install MSI, Install Uploaded MSI, Uninstall MSI
- Install MSP, Install Uploaded MSP
- Install Font, Install Uploaded Font
- Start Process, Start Uploaded Process
- Create Registry Key, Delete Registry Key
- Set Registry Value, Delete Registry Value

To set 'Elevated user' as the context for an action:

1. From the Application Workspace **Packages** page, select a package and choose the **Actions** tab.

2. Open the **Actions** set editor for a supported action type.

3. On the **Advanced** tab, as the Execution or User **Context**, select 'Elevated user' from the drop-down.

4. Click **Confirm** to save the setting.

When you select 'Elevated User' as the context, the Action editor displays an informational message:

"This action will be executed with administrative permissions. Actions running with elevated permissions can affect system settings and security. Use with caution and only when required."