Recast

Application Workspace 4.5 Features

Last Modified on 2026-09-01

These features are included in each Application Workspace version 4.5 release:

Application Settings Follow End Users

Application Workspace administrators can now enable end users to retain some application preferences across devices and sessions. As an administrator, you specify the exact application settings to save and restore for end users and then link those settings to one or more packages. For end users, the result is a consistent, uninterrupted experience without the need to reconfigure settings for different devices or sessions.

Application settings that an administrator can configure for roaming:

- Folder Tree
- Folder
- File
- Registry Tree
- Registry Key
- Registry Value

NOTE: To retain application settings correctly, end users must launch the application using the Application Workspace Smart Icon.

For detailed information about this feature, including how to create application settings and link them to packages, seeApp Settings.

The App Settings feature is available to Application Workspace customers with Access Manager licensing.

Known Issues

- **Folder Exclusions**: The App Settings feature may incorrectly capture and restore settings that are within an excluded subfolder.
- **Wildcard Support**: Wildcards (`*`) do not resolve as dynamic path placeholders, meaning that you must define the exact path to a file or folder. To work around the issue, you can, where applicable, use environment variables such as `%USERPROFILE%` . The next release will add support for wildcards in folder/file paths.
- **MSIX/AppV restore integration**: Restore operations work for standard applications but not for MSIX or AppV applications in the documented scenario.
- **RPC**: Events are not logged.
- **Hive Key Support**: `HKCU\Software<App>` is not supported. For now, use `HKEY_CURRENT_USER\Software<App>` .

Grant Elevated User Permissions to Run Windows Actions

Application Workspace administrators can now temporarily elevate the privileges granted to non-administrator users to allow those users to run specific actions as the current logged-on user.

As an administrator, this means that you can elevate privileges without needing to manually add the user to (and remove them from) the local Administrator group. You'll also be spared from developing workaround scripts to enable users with standard permissions to run Windows actions that require elevation.

As an Application Workspace user who does not have local admin rights, you'll be able to execute an action that requires elevated privileges and have it complete successfully instead of failing because of a lack of permissions.

Actions that an administrator can enable with user privilege elevation:

- 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

For instructions on enabling this feature and configuring an action to run in the context of an elevated user, see Temporarily Elevate User Privileges to Run Actions.

To learn about security features and potential risks associated with user privilege elevation, see Security Considerations.